3Com® Unified Gigabit Wireless PoE Switch 24

Command Reference Guide

3CRUS2475

www.3Com.com
Part No. 10015248 Rev. AA
Published October 2006

3Com Corporation
350 Campus Drive
Marlborough,
MA 01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a ”commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

ntel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

USING THE CLI

AAA COMMANDS

ACL Commands

Address Table Commands

Ethernet Configuration Commands

LINE COMMANDS

PHY DIAGNOSTICS COMMANDS

Port Channel Commands

QoS Commands

Clock Commands

RMON Commands

IGMP Snooping Commands

LACP Commands

Power over Ethernet commands

Spanning-Tree Commands

CONFIGURATION AND IMAGE FILE COMMANDS

RADIUS COMMAND

PORT MONITOR COMMANDS

SNMP COMMANDS

IP ADDRESS COMMANDS

Management ACL Commands

Wireless Rogue AP Commands

Wireless ESS Commands

WIRELESS AP GENERAL COMMANDS

SSH COMMANDS

WEB SERVER COMMANDS

TACACS+ COMMANDS

SYSLOG COMMANDS

WIRELESS AP BSS COMMANDS

SYSTEM MANAGEMENT COMMANDS

USER INTERFACE COMMANDS

GVRP Commands

VLAN Commands

802.1x Commands

WIRELESS AP RADIO COMMANDS

WIRELESS WLAN COMMANDS

TROUBLESHOOTING

1 USING THE CLI

Overview

This document describes the Command Line Interface (CLI) used to manage the 3Com Unified Gigabit Wireless PoE switch.

Most of the CLI commands are applicable to all devices.

This chapter describes how to start using the CLI and the CLI command editing features.

CLI Command Modes

Introduction

To assist in configuring the device, the Command Line Interface (CLI) is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark **?** at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode, a specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: *User EXEC* mode, *Privileged EXEC* mode, *Global Configuration* mode, and *Interface Configuration* mode.

When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands are available in User EXEC mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode gives access to commands that are restricted on User EXEC mode and provides access to the device Configuration mode.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures specific interfaces in the device.

User EXEC Mode

After logging into the device, the user is automatically in User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device host name followed by the angle bracket (>).

```
Console>
```

The default host name is Console unless it has been changed using the **hostname** command in the Global Configuration mode.

Privileged EXEC

Privileged access is password protected to prevent unauthorized use because many of the Privileged commands set operating system parameters. The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode. To enter the Privileged EXEC mode from the User EXEC mode, perform the following steps:

1 At the prompt enter the **enable** command and press <Enter>. A password prompt is displayed.

2 Enter the password and press <Enter>. The password is displayed as *. The Privileged EXEC mode prompt is displayed. The Privileged EXEC mode prompt consists of the device host name followed by **#**.

3 To return from the Privileged EXEC mode to the User EXEC mode, use the **disable** command.

The following example illustrates how to access the Privileged EXEC mode and return to the User EXEC mode:

```
Console> enable
Enter Password: ******
Console#
Console# disable
Console>
```

4 The **exit** command is used to return from any mode to the previous mode except when returning to the User EXEC mode from the Privileged EXEC mode. For example, the **exit** command is used to return from the Interface Configuration mode to the Global Configuration mode.

Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface. The **configure** Privileged EXEC mode command is used to enter the Global Configuration mode.

To enter the Global Configuration mode perform the following steps:

1. At the Privileged EXEC mode prompt, enter the **configure** command and press <Enter>. The Global Configuration mode prompt is displayed. The Global Configuration mode prompt consists of the device host name followed by (config) and **#**.

```
Console(config)#
```

2. To return from the Global Configuration mode to the Privileged EXEC mode, the user can use one of the following commands:

   - **exit**
   - **end**
   - **Ctrl+Z**

The following example illustrates how to access the Global Configuration mode and return to the Privileged EXEC mode:

```
Console#
Console# configure
Console(config)# exit
Console#
```

Interface Configuration and Specific Configuration Modes

Interface Configuration mode commands modify specific interface operations. The following are the Interface Configuration modes:

- **Line Interface** — Contains commands to configure the management connections. These include commands such as line timeout settings, etc. The **line** Global Configuration mode command is used to enter the Line Configuration command mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The **vlan database** Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.
- **Management Access List** — Contains commands to define management access-lists. The **management access-list** Global Configuration mode command is used to enter the Management Access List Configuration mode.

- **Ethernet** — Contains commands to manage port configuration. The **interface ethernet** Global Configuration mode command is used to enter the Interface Configuration mode to configure an Ethernet type interface.
- **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The **interface port-channel** Global Configuration mode command is used to enter the Port Channel Interface Configuration mode.
- **SSH Public Key-chain** — Contains commands to manually specify other device SSH public keys. The **crypto key pubkey-chain ssh** Global Configuration mode command is used to enter the SSH Public Key-chain Configuration mode.
- **QoS —** Contains commands related to service definitions. The **qos** Global Configuration mode command is used to enter the QoS services configuration mode.
- **MAC Access-List** — Configures conditions required to allow traffic based on MAC addresses. The **mac access-list** Global Configuration mode command is used to enter the MAC access-list configuration mode.

Starting the CLI

The device can be managed over a direct connection to the device console port or via a Telnet connection. The device is managed by entering command keywords and parameters at the prompt. Using the device command-line interface (CLI) is very similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure that the device has a defined IP address, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

The following instructions are for use on the console line only.

To start using the CLI, perform the following steps:

1 Connect the DB9 null-modem or cross over cable to the RS-232 serial port of the device to the RS-232 serial port of the terminal or computer running the terminal emulation application.

   a Set the data format to 8 data bits, 1 stop bit, and no parity.

   b Set Flow Control to **none**.

   c Under **Properties**, select **VT100 for Emulation** mode.

   d Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** (not **Windows keys**).

   Note: When using HyperTerminal with Microsoft® Windows 2000, ensure that Windows® 2000 Service Pack 2 or later is installed.With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

2 Enter the following commands to begin the configuration procedure:

```
Console> enable
Console# configure
Console(config)#
```

3 Configure the device and enter the necessary commands to complete the required tasks.

4 When finished, exit the session with the **exit** command.

   When a different user is required to log onto the system, use the **login** Privileged EXEC mode command. This effectively logs off the current user and logs on the new user.

Editing Features

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command **show interfaces status ethernet g11**, **show**, **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **g11** specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)# username admin password alansmith
```

When working with the CLI, the command options are not displayed. The command is not selected from a menu, but is manually entered. To see what commands are available in each mode or within an Interface Configuration, the CLI does provide a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request help is **?**.

There are two instances where help information can be displayed:

- **Keyword lookup** — The character **?** is entered in place of a command. A list of all valid commands and corresponding help messages are is displayed.
- **Partial keyword lookup** — If a command is incomplete and or the character **?** is entered in place of a parameter. The matched keyword or parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Nomenclature
- Keyboard Shortcuts

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a *First In First Out (FIFO)* basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Table 1: Keyword	Table 2: Description

Up-arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see **history**.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see **history size**.

To display the history buffer, see **“show history”**.

Negating the Effect of Commands

For many configuration commands, the prefix keyword **no** can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If the command entered is incomplete, invalid or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing the <Tab> button, an incomplete command is entered. If the characters already entered are not enough for the system to identify a single matching command, press **?** to display the available commands matching the characters already entered.

Nomenclature

When referring to an Ethernet port in a CLI command, the following format is used:

- For an Ethernet port: *Ethernet_type port_number*

The Ethernet type may be Gigabit Ethernet (indicated by “g”).

For example, g3 stands for Gigabit Ethernet port 3 on the device.

The ports may be described on an individual basis or within a range. Use format *port number-port number* to specify a set of consecutive ports and *port number, port number* to indicates a set of non-consecutive ports. For example, g1-3 stands for Gigabit Ethernet ports 1, 2 and 3, and g1,5 stands for Gigabit Ethernet ports 1 and 5.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Table 3: Keyboard Key	**Table 4: Description**
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace key	Deletes one character left to the cursor position.

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the | character. One option must be selected. For example: **flowcontrol** {**auto|on|off**} means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Indicates an individual key on the keyboard. For example, <Enter> indicates the **Enter** key.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
`Screen Display`	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.

It is the user’s responsibility to ensure that the text copied into the device consists of legal commands only.

This feature is dependent on the baud rate of the device.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.
- The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device.

2 AAA COMMANDS

aaa authentication login

The **aaa authentication login** Global Configuration mode command defines login authentication. To restore defaults, use the **no** form of this command.

Syntax

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name* — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters)
- *method1* [*method2*...] — Specify at least one method from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **aaa authentication login** *list-name local.*

On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures the authentication login.

```
Console(config)# aaa authentication
login default radius tacacs enable line local none
```

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command defines authentication method lists for accessing higher privilege levels. To restore defaults, use the **no** form of this command.

Syntax

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable {**default** | *list-name*}

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.

- *list-name* — Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-12 characters)
- *method1* [*method2*...] — Specify at least one method from the following list:

Keyword	**Description**
enableT	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication. Uses username $enabx$., where x is the privilege level.
tacacs	Uses the list of all TACACS+ servers for authentication. Uses username "$enabx$." where x is the privilege level.

Default Configuration

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable** *default enable*.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable** *default enable none*.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable** *default* requests sent by the device to a RADIUS or TACACS+ server include the username $enabx$., where x is the requested privilege level.

Example

The following example sets the enable password for authentication when accessing higher privilege levels.

```
Console(config)# aaa authentication enable default enable
```

login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote telnet or console. To restore the default configuration specified by the **aaa authentication login** command, use the **no** form of this command.

Syntax

Login authentication {**default** | *list-name*}

no login authentication

Parameters

- **default** — Uses the default list created with the **aaa authentication login** command.
- *list-name* — Uses the indicated list created with the **aaa authentication login** command.

Default Configuration

Uses the default set with the command **aaa authentication login**.

Command Mode

Line Configuration mode

User Guidelines

To change (or rename) an authentication method, use the negate command and create a new rule with the new method name.

Example

The following example specifies the default authentication method for a console.

```
Console(config)# line console
Console(config-line)# login authentication default
```

enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote Telnet or console. To restore the default configuration specified by the **aaa authentication enable** command, use the **no** form of this command.

Syntax

enable authentication {**default** | *list-name*}

no enable authentication

Parameters

- **default** — Uses the default list created with the **aaa authentication enable** command.
- *list-name* — Uses the indicated list created with the **aaa authentication enable** command.

Default Configuration

Uses the default set with the **aaa authentication enable** command.

Command Mode

Line Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the default authentication method when accessing a higher privilege level from a console.

```
Console(config)# line console
Console(config-line)# enable authentication default
```

ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server users. To restore the default configuration, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2*...]

no ip http authentication

Parameters

- *Method1* [*method2*...] — Specify at least one method from the following list:

Keyword	**Description**
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip http authentication** *local.*

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures the HTTP authentication.

```
Console(config)# ip http authentication radius tacacs local
none
```

ip https authentication

The **ip https authentication** Global Configuration mode command specifies authentication methods for HTTPS server users. To restore the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2*...]

no ip https authentication

Parameters

- *method1* [*method2*...] — Specify at least one method from the following list:

Keyword	**Source or Destination**
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip https authentication** *local*.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures HTTPS authentication.

```
Console(config)# ip https authentication radius tacacs local
none
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the authentication configuration.

```
Console# show authentication methods
Login Authentication Method Lists
---------------------------------
Default: Local

Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None

Line                   Login Method List     Enable Method List
--------------         -----------------     ------------------
Console                Default               Default
Telnet                 Default               Default
SSH                    Default               Default

http: Local
https: Local
dot1x:
```

password

The **password** Line Configuration mode command specifies a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

Parameters

- *password* — Password for this level. (Range: 1-159 characters)
- **encrypted** — Encrypted password to be entered, copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration mode

User Guidelines

If a password is defined as encrypted, the required password length is 32 characters.

Example

The following example specifies the password called ‘secret’ on a console.

```
Console(config)# line console
Console(config-line)# password secret
```

enable password

The **enable password** Global Configuration mode command sets a local password to control access to user and privilege levels. To remove the password requirement, use the **no** form of this command.

Syntax

enable password [**level** *level*] *password* [**encrypted**]

no enable password [**level** *level*]

Parameters

- *password* — Password for this level. (Range: 1-159 characters)
- *level* — Level for which the password applies. If not specified the level is 15
  (Range: 1-15).
- **encrypted** — Encrypted password entered, copied from another device configuration.

Default Configuration

No enable password is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a local level 15 password called ‘secret’ to control access to user and privilege levels. .

```
Console(config)# enable password secret level 15
```

username

The **username** Global Configuration mode command creates a user account in the local database. To remove a user name, use the **no** form of this command.

Syntax

username *name* [**password** *password*] [**level** *level*] [**encrypted**]

no username *name*

Parameters

- *name* — The name of the user. (Range: 1-20 characters)
- *password* — The authentication password for the user. (Range: 1-159 characters)
- *level* — The user level (Range: 1-15). If a level is not specified, the level is automaically set to 1.

- **encrypted** — Encrypted password entered, copied from another device configuration.

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

User Guidelines

User account can be created without a password.

Example

The following example configures user called bob with password ‘lee’ and user level 15 to the system.

```
Console(config)# username bob password lee level 15
```

3 ACL COMMANDS

ip access-list

The **ip access-list** Global Configuration mode command enables the IP-Access Configuration mode and creates Layer 3 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

ip access-list *name*

no ip access-list name

Parameters

- *name* — Specifies the name of the ACL. (Range: 0-32 characters)

Default Configuration

The default for all ACLs is deny-all.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to create an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)#
```

permit (ip)

The **permit IP**-Access List Configuration mode command permits traffic if the conditions defined in the permit statement match.

Syntax

permit {*any* | *protocol*} {**any** | {*source source-wildcard*}} {**any |** {*destination destination-wildcard*}} [**dscp** *dscp numbe*r | **ip-precedence** *ip-precedence*]

permit-icmp {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**any** | *icmp-type*} {**any** | *icmp-code*} [**dscp** *number* | **ip-precedence** *number*]

permit-igmp {any | {*source source-wildcard*}} {**any** | {de*stination destination-wildcard*}} {**any** | *igmp-type*} [**dscp** *number* | **ip-precedence** *number*]

permit-tcp {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** |{*destination destination-wildcard*}} {**any** | *destination-port*} **[dscp** *number* | **ip-precedence** *number*] [**flags** *list-of-flags*]

permit-udp {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** | {*destination destination-wildcard*}} {**any** | *destination-port*} [**dscp** *number* | **ip-precedence** *number*]

Parameters

- *source* — Specifies the source IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — Specifies wildcard to be applied to the source IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination* — Specifies the destination IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — Specifies wildcard to be applied to the destination IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *protocol* — Specifies the abbreviated name or number of an IP protocol. (Range: 0-255)

The following table lists the protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ipinip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Ipv6 protocol	ipv6	41
Routing Header for IPv6	ipv6-route	43
Fragment Header for IPv6	ipv6-frag	44
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
ICMP for IPv6	ipv6-icmp	58
EIGRP routing protocol	eigrp	88
Open Shortest Path Protocol	ospf	89
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115
ISIS over IPv4	isis	124
(any IP protocol)	any	(25504)

- **dscp** — Indicates matching the dscp number with the packet dscp value.
- **ip-precedence** — Indicates matching ip-precedence with the packet ip-precedence value.
- *icmp-type* — Specifies an ICMP message type for filtering ICMP packets. Enter a value or one of the following values: **echo-reply, destination-unreachable, source-quench, redirect,**

alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, ipv6-where-are-you, ipv6-i-am-here, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip and **photuris**. (Range: 0-255)

- *icmp-code* — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. (Range: 0-255)
- *igmp-type* — IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: **dvmrp, host-query, host-report, pim** or **trace**. (Range: 0-255)
- *destination-port* — Specifies the UDP/TCP destination port. (Range: 0-65535)
- *source-port* — Specifies the UDP/TCP source port. (Range: 0-65535)
- li*st-of-flags* — Specifies a list of TCP flags that can be triggered. If a flag is set, it is prefixed by "+". If a flag is not set, it is prefixed by "-". The possible values are: **+urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn** and **-fin**. The flags are concatenated into one string. For example: +fin-ack.

Default Configuration

No IPv4 ACL is defined.

Command Mode

IP-Access List Configuration mode

User Guidelines

Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# permit rsvp 192.1.1.1 0.0.0.0 any dscp56
```

deny (IP)

The **deny** IP-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny [**disable-port**] {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp number* | ***ip-precedence*** *ip-precedence*]

deny-icmp

deny-igmp

deny-tcp

deny-udp

Parameters

- **disable-port** — Specifies that the port is disabled.
- *source* — Specifies the IP address or host name from which the packet was sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination* — Specifies the IP address or host name to which the packet is being sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *protocol* — Specifies the abbreviated name or number of an IP protocol. The following table lists protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Ipv6 protocol	ipv6	41
Routing Header for IPv6	ipv6-route	43
Fragment Header for IPv6	ipv6-frag	44
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
ICMP for IPv6	ipv6-icmp	58
EIGRP routing protocol	eigrp	88
Open Shortest Path Protocol	ospf	89
IP-within-IP Encapsulation Protocol	ipip	94
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115
ISIS over IPv4	isis	124
(any IP protocol)	any	(25504)

- **dscp** — Indicates matching the dscp number with the packet dscp value.
- **ip-precedence** — Indicates matching ip-precedence with the packet ip-precedence value.

Default Configuration

This command has no default configuration

Command Mode

IP-Access List Configuration mode

User Guidelines

Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the defined conditions are denied.

Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# deny rsvp 192.1.1.1 0.0.0.255 any
```

mac access-list

The **mac access-list** Global Configuration mode command enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

mac access-list *name*

no mac access-list *name*

Parameters

- *name* — Specifies the name of the ACL. (Range: 0-32 characters)

Default Configuration

The default for all ACLs is deny all.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to create a MAC ACL.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)#
```

permit (MAC)

The **permit** MAC-Access List Configuration mode command defines permit conditions of an MAC ACL.

Syntax

permit {**any** | {**host** *source source-wildcar*d} **any** | {*destination destination-wildc*ard}} **[vlan** v*lan-id*] [**cos** *cos cos-wildcar*d] [**ethtype** *eth-typ*e]

Parameters

- *source* — Specifies the source MAC address of the packet.
- *source-wildcard* — Specifies wildcard bits to be applied to the source MAC address. Use 1s in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is being sent.
- *destination-wildcard* — Specifies wildcard bits to be applied to the destination MAC address. Use 1s in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan. (Range: 0-4095)
- *cos* — Specifies the Class of Service (CoS) for the packet. (Range: 0-7)
- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the Ethernet type of the packet .(Range: 0-65535)

Default Configuration

No MAC ACL is defined.

Command Mode

MAC-Access List Configuration mode

User Guidelines

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

Example

The following example shows how to create a MAC ACL with permit rules.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any
vlan 6
```

deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny [**disable-port**] {**any** | {source source-wildcard} {**any** | {destination destination- wildcard}}[**vlan** vlan-id] [**cos** cos cos-wildcard] [**ethtype** eth-type]

Parameters

- **disable-port** — Indicates that the port is disabled if the statement is deny.
- *source* — Specifies the MAC address of the host from which the packet was sent.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is being sent.
- *destination-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan.
- *cos* — Specifies the packets's Class of Service (CoS).

- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the packet’s Ethernet type.

Default Configuration

This command has no default configuration.

Command Mode

MAC-Access List Configuration mode

User Guidelines

MAC BPDU packets cannot be denied.

This command defines an Access Control Element (ACE). An ACE can only be removed by deleting the ACL, using the **no mac access-list** Global Configuration mode command. Alternatively, the Web-based interface can be used to delete ACEs from an ACL.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

Example

The following example shows how to create a MAC ACL with deny rules on a device.

```
Console(config)# mac access-list macl1
Console (config-mac-acl)# deny 6:6:6:6:6:6:0:0:0:0:0:0 any
```

service-acl

The **service-acl** Interface Configuration mode command applies an ACL to the input interface. To detach an ACL from an input interface, use the **no** form of this command.

Syntax

service-acl {**input** *acl-name*}

no service-acl {**input**}

Parameters

- *acl-name*—Specifies the ACL to be applied to the input interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface (Ethernet, port-channel) Configuration mode.

User Guidelines

In advanced mode, when an ACL is bound to an interface, the port trust mode is set to trust 12-13 and not to 12.

Example

The following example binds (services) an ACL to VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# service-acl input macl1
```

show access-lists

The **show access-lists** Privileged EXEC mode command displays access control lists (ACLs) defined on the device.

Syntax

show access-lists [*name*]

Parameters

- *name* — The name of the ACL.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays access lists defined on a device.

```
Console# show access-lists
IP access list ACL1
permit ip host 172.30.40.1 any
permit rsvp host 172.30.8.8 any
```

show interfaces access-lists

The **show interfaces access-lists** Privileged EXEC mode command displays access lists applied on interfaces.

Syntax

show interfaces access-lists [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays ACLs applied to the interfaces of a device:

```
Console# show interfaces access-lists


Interface                         Input ACL
---------                         ---------
g1                                ACL1
g1                                ACL3
```

4 ADDRESS TABLE COMMANDS

bridge address

The **bridge address** Interface Configuration (VLAN) mode command adds a MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of this command.

Syntax

bridge address *mac-address* {**ethernet** *interface* | **port-channel** *port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]

no bridge address [*mac-address*]

Parameters

- *mac-address* — A valid MAC address.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- **permanent** — The address can only be deleted by the no bridge address command.
- **delete-on-reset** — The address is deleted after reset.
- **delete-on-timeout** — The address is deleted after "age out" time has expired.
- **secure** — The address is deleted after the port changes mode to unlock learning (no port security command). This parameter is only available when the port is in the learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port 1 to the bridge table.

```
Console(config)# interface vlan 2
Console(config-if)# bridge address 3aa2.64b3.a245 ethernet g16
permanent
```

bridge multicast filtering

The **bridge multicast filtering** Global Configuration mode command enables filtering multicast addresses. To disable filtering multicast addresses, use the **no** form of this command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Filtering multicast addresses is disabled. All multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

If multicast devices exist on the VLAN, do not change the unregistered multicast addresses state to drop on the switch ports.

If multicast devices exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all multicast packets to the multicast switches.

Example

In the folowing example, bridge multicast filtering is enabled.

```
Console(config)# bridge multicast filtering
```

bridge multicast address

The **bridge multicast address** Interface Configuration (VLAN) mode command registers a MAC-layer multicast address in the bridge table and statically adds ports to the group. To unregister the MAC address, use the **no** form of this command.

Syntax

bridge multicast address *{mac-multicast-address* | *ip-multicast-address}*

bridge multicast address *{mac-multicast-address* | *ip-multicast-address}* [**add** | **remove**] {**ethernet** *interface-list* | *port-channel* p**ort-channel**-*number-list}*

no bridge multicast address *{mac-multicast-address* | *ip-multicast-address}*

Parameters

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip- multicast-address* — A valid IP multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

Default Configuration

No multicast addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.

Static multicast addresses can only be defined on static VLANs.

Example

The following example registers the MAC address:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
add ethernet g1, g2
```

bridge multicast forbidden address

The **bridge multicast forbidden address** Interface Configuration (VLAN) mode command forbids adding a specific multicast address to specific ports. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address}*

Parameters

- **add** — Adds ports to the group.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip- multicast-address* — A valid IP multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Modes

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the multicast group should be registered.

Example

In this example, MAC address 0100.5e02.0203 is forbidden on port g9 within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 0100.5e.02.0203
Console(config-if)# bridge multicast forbidden address
0100.5e02.0203 add ethernet g9
```

bridge multicast forward-all

The **bridge multicast forward-all** Interface Configuration (VLAN) mode command enables forwarding all multicast packets on a port. To restore the default configuration, use the **no** form of this command.

Syntax

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forward-all

Parameters

- **add** — Force forwarding all multicast packets.
- **remove** — Do not force forwarding all multicast packets.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separates nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all multicast packets on port 8 are forwarded.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add
ethernet g8
```

bridge multicast forbidden forward-all

The **bridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command forbids a port to be a forward-all-multicast port. To restore the default configuration, use the **no** form of this command.

Syntax

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden forward-all

Parameters

- **add** — Forbids forwarding all multicast packets.
- **remove** — Does not forbid forwarding all multicast packets.
- *interface-list* — Separates nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separates nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping dynamically discovers multicast device ports. When a multicast device port is discovered, all the multicast packets are forwarded to it unconditionally.

This command prevents a port from becoming a multicast device port.

Example

In this example, forwarding all multicast packets to g1 with VLAN 2 is forbidden.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all
add ethernet g1
```

bridge aging-time

The **bridge aging-time** Global Configuration mode command sets the address table aging time. To restore the default configuration, use the **no** form of this command.

Syntax

bridge aging-time seconds

no bridge aging-time

Parameters

- *seconds* — Time in seconds. (Range: 10-630 seconds)

Default Configuration

The default setting is 300 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the bridge aging time is set to 250 seconds.

```
Console(config)# bridge aging-time 250
```

clear bridge

The **clear bridge** Privileged EXEC mode command removes any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the bridge tables are cleared.

```
Console# clear bridge
```

port security

The **port security** Interface Configuration mode command locks the port to block unknown traffic and prevent the port from learning new addresses. To restore the default configuration, use the **no** form of this command.

Syntax

port security [forward | **discard** | **discard-shutdown**] **[trap** *seconds*] [**max**]

no port security

Parameters

- **forward** — Forwards packets with unlearned source addresses, but does not learn the address.
- **discard** — Discards packets with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown** — Discards packets with unlearned source addresses. The port is also shut down.
- **trap** *seconds* — Sends SNMP traps and defines the minimum amount of time in seconds between consecutive traps. (Range: 1-1000000)
- **max** — Maximum number of addresses that can be learned on the interface. (Range: 1-128)

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, port g1 forwards all packets without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```
Console(config)# interface ethernet g1
Console(config-if)# port security forward trap 100
```

port security mode

The **port security mode** Interface Configuration mode command configures the port security mode. To restore the default configuration, use the **no** form of this command.

Syntax

port security mode {**lock** | **mac-addresses**}

no port security mode

Parameters

- **lock** — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **mac-addresses** — Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number addresses allowed on the port. Relearning and aging are enabled.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, port security mode is set to dynamic for Ethernet interface g7.

```
Console(config)# interface ethernet g7
Console(config-if)# port security mode mac-addresses
```

port security routed secure-address

The **port security routed secure-address** Interface Configuration (Ethernet, port-channel) mode command adds a MAC-layer secure address to a routed port. Use the **no** form of this command to delete a MAC address.

Syntax

port security routed secure-address *mac-address*

n**o port security routed secure-address** *mac-address*

Parameters

- *mac-address* — A valid MAC address.

Default Configuration

No addresses are defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode. Cannot be configured for a range of interfaces (range context).

User Guidelines

The command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

In this example, the MAC-layer address 66:66:66:66:66:66 is added to port g1.

```
Console(config)# interface ethernet g1
Console(config-if)# port security routed secure-address
66:66:66:66:66:66
```

show bridge address-table

The **show bridge address-table** Privileged EXEC mode command displays all entries in the bridge-forwarding database.

Syntax

show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number* | **address** *mac address*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- *mac address* — A valid MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Internal usage VLANs (VLANs that are automatically allocated on ports with a defined Layer 3 interface) are presented in the VLAN column by a port number and not by a VLAN ID.

"Special" MAC addresses that were not statically defined or dynamically learned are displayed in the MAC address table. This includes, for example, MAC addresses defined in ACLS.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table


Aging time is 300 sec


interface        mac address      Port             Type

---------        --------------   ----             -------

1                00:60:70:4C:73   g8               dynamic
                 :FF

1                00:60:70:8C:73   g8               dynamic
                 :FF

200              00:10:0D:48:37   g9               static
                 :FF
```

show bridge address-table static

The **show bridge address-table** static Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

Syntax

show bridge address-table static [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters \

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table static


Aging time is 300 sec


vlan           mac address    port           type

----           -------------- ----           --------------
               ---                           ---

1              00:60:70:4C:73 g8             Permanent
               :FF

1              00:60.70.8C.73 g8             delete-on-time
               :FF                           out

200            00:10:0D:48:37 g9             delete-on-rese
               :FF                           t
```

show bridge address-table count

The **show bridge address-table** count Privileged EXEC mode command displays the number of addresses present in the Forwarding Database.

Syntax

show bridge address-table count [**vlan** *vlan*] [**ethernet** *interface-number* | **port-channel** *port-channel-number*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the number of addresses present in all VLANs are displayed.

```
Console# show bridge address-table count


Capacity: 8192

Free: 8083

Used: 109


Secure addresses: 2

Static addresses: 1

Dynamic addresses: 97

Internal addresses: 9
```

show bridge multicast address-table

The **show bridge multicast address-table** Privileged EXEC mode command displays multicast MAC address or IP address table information.

Syntax

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*] [**format ip | format mac]**

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip-multicast-address* — A valid IP multicast address.
- **format** *ip / mac* — Multicast address format. Can be **ip** or **mac**. If the format is unspecified, the default is **mac**.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is in the range of 0100.5e00.0000-0100.5e7f.ffff.

Example

In this example, multicast MAC address and IP address table information is displayed.

```
Console# show bridge multicast address-table


Vlan             MAC Address      Type             Ports
----             --------------   -------          ----------
1                01:00:5e:02:02   static           g1, g2
                 :03
```

```
19               01:00:5e:02:02   static           g1-8
                 :08
19               00:00:5e:02:02   dynamic          g9-11
                 :08

Forbidden ports for multicast addresses:

Vlan             MAC Address      Ports
----             --------------   -----
1                01:00:5e:02:02   8
                 :03
19               01:00:5e:02:02   8
                 :08

Console# show bridge multicast address-table format ip

Vlan             IP/MAC Address   Type             Ports
----             --------------   ------           ---------
                 ---
1                224-239.130|2.   static           g1, g2
                 2.3
19               224-239.130|2.   static           g1-8
                 2.8
19               224-239.130|2.   dynamic          g9-11
                 2.8

Forbidden ports for multicast addresses:

Vlan             IP/MAC Address   Ports
----             --------------   ------
                 ---
1                224-239.130|2.   g8
                 2.3
19               224-239.130|2.   g8
                 2.8
```

A multicast MAC address maps to multiple IP addresses as shown above.

show bridge multicast filtering

The **show bridge multicast filtering** Privileged EXEC mode command displays the multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the multicast configuration for VLAN 1 is displayed.

```
Console# show bridge multicast filtering 1


Filtering: Enabled

VLAN: 1


Port         Static        Status

----         ---------     ---------

g1                         Filter

g2                         Filter

g3           -             Filter
```

show ports security

The **show ports security** Privileged EXEC mode command displays the port-lock status.

Syntax

show ports security [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all classes of entries in the port-lock status are displayed:

```
Console# show ports security


Port     Status   Learni   Action   Maximu   Trap     Frequency
                  ng                m

----     ------   ------   ------   ------   ------   ---------
         -        --       -        -        -

g1       Locked   Dynami   Discar   3        Enable   100
                  c        d
```

```
g2      Unlock  Dynami  -       28      -       -
        ed      c

g3      Locked  Disabl  Discar  8       Disabl  -
                ed      d,              e
                        Shutdo
                        wn
```

The following table describes the fields shown above.

Field	Description
Port	The port number.
Status	The values are: Locked/Unlocked.
Learning	The learning mode.
Action	Action on violation.
Maximum	The maximum number of addresses that can be associated on this port in theStatic Learning mode or in the Dynamic Learning mode.
Trap	Sends traps in case of a violation.
Frequency	The minimum time interval between consecutive traps.

show ports security addresses

The **show ports security addresses** Privileged EXEC mode command displays the current dynamic addresses in locked ports.

Syntax

show ports security addresses [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

This example displays dynamic addresses in all currently locked ports.

```
Console# show ports security addresses


Port          Status        Learning      Current       Maximum
----          --------      --------      -------       -------
g1            Disabled      Lock          -             1
g2            Disabled      Lock          -             1
g3            Enabled       Max-addres    0             1
                            ses
g4            Port is a member in port-channel ch1
g5            Disabled      Lock          -             1
6             Enabled       Max-addres    0             10
                            ses
ch1           Enabled       Max-addres    0             50
                            ses
ch2           Enabled       Max-addres    0             128
                            ses
```

This example displays dynamic addresses in the currently locked port 1.

```
Console# show ports security addresses ethernet 1


Port          Status        Learning      Current       Maximum
----          --------      --------      -------       -------
g1            Disabled      Lock          -             1
```

5 ETHERNET CONFIGURATION COMMANDS

interface ethernet

The **interface ethernet** Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

Parameters

- *interface* — Valid Ethernet port. Elana

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables configuring Ethernet port g18.

```
Console(config)# interface ethernet g18
```

interface range ethernet

The **interface range ethernet** Global Configuration mode command configures multiple Ethernet type interfaces at the same time.

Syntax

interface range ethernet {*port-list* | **all**}

Parameters

- *port-list* — List of valid ports. Where more than one port is listed, separate the nonconsecutive ports with a comma and no spaces, use a hyphen to designate a range of ports and group a list separated by commas in brackets.
- **all** — All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example

The following example shows how ports g18 to g20 and g1 to g24 are grouped to receive the same command.

```
Console(config)# interface range ethernet g18-g20,g1-g24
Console(config-if)#
```

shutdown

The **shutdown** Interface Configuration (Ethernet, port-channel) mode command disables an interface. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables Ethernet port g5 operations.

```
Console(config)# interface ethernet g5
Console(config-if)# shutdown
```

The following example restarts the disabled Ethernet port.

```
Console(config)# interface ethernet g5
Console(config-if)# no shutdown
```

description

The **description** Interface Configuration (Ethernet, port-channel) mode command adds a description to an interface. To remove the description, use the **no** form of this command.

Syntax

description *string*

no description

Parameters

- *string* — Comment or a description of the port to enable the user to remember what is attached to the port. (Range: 1-64 characters)

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a description to Ethernet port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# description "RD SW#3"
```

speed

The **speed** Interface Configuration (Ethernet, port-channel) mode command configures the speed of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

Syntax

speed {10 | 100 | 1000| 10000}

Parameters

- **10** — Forces10 Mbps operation.
- **100** — Forces 100 Mbps operation.
- **1000** — Forces 1000 Mbps operation.
- **10000** — Forces 10000 Mbps operation.

Default Configuration

Maximum port capability

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the speed operation of Ethernet port g5 to 100 Mbps operation.

```
Console(config)# interface ethernet g5
Console(config-if)# speed 100
```

duplex

The **duplex** Interface Configuration (Ethernet) mode command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

Syntax

duplex {half | full}

Parameters

- **no** duplex
- **half** — Forces half-duplex operation
- **full** — Forces full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

When configuring a particular duplex mode on the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

Example

The following example configures the duplex operation of Ethernet port g1 to full duplex operation.

```
Console(config)# interface ethernet g1
Console(config-if)# duplex full
```

negotiation

The **negotiation** Interface Configuration (Ethernet, port-channel) mode command enables auto-negotiation operation for the speed and duplex parameters of a given interface. To disable auto-negotiation, use the **no** form of this command.

Syntax

negotiation [*capability1 [capability2…capability5*]]

no negotiation

Parameters

- **capability** — Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f)

Default Configuration

Auto-negotiation is enabled.

If unspecified, the default setting is to enable all capabilities of the port.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If capabilities were specified when auto-negotiation was previously entered, not specifying capabilities when currently entering auto-negotiation overrides the previous configuration and enables all capabilities.

Example

The following example enables auto-negotiation on Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# negotiation
```

flowcontrol

The **flowcontrol** Interface Configuration (Ethernet, port-channel) mode command configures flow control on a given interface. To disable flow control, use the **no** form of this command.

Syntax

flowcontrol {auto | on | off}

no flowcontrol

Parameters

- **auto** — Indicates auto-negotiation
- **on** — Enables flow control.
- **off** — Disables flow control.

Default Configuration

Flow control is off.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Negotiation should be enabled for flow control auto.

Example

In the following example, flow control is enabled on port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# flowcontrol on
```

mdix

The **mdix** Interface Configuration (Ethernet) mode command enables cable crossover on a given interface. To disable cable crossover, use the **no** form of this command.

Syntax

mdix {on | auto}

no mdix

Parameters

- **on** — Manual mdix is enabled.
- **auto** — Automatic mdi/mdix is enabled.

Default Configuration

The default setting is **on**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Auto: All possibilities to connect a PC with cross or normal cables are supported and are automatically detected.

On: It is possible to connect to a PC only with a normal cable and to connect to another device only with a cross cable.

No: It is possible to connect to a PC only with a cross cable and to connect to another device only with a normal cable.

Example

In the following example, automatic crossover is enabled on port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# mdix auto
```

clear counters

The **clear counters** Privileged EXEC mode command clears statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. Elana
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the counters for interface 1 are cleared.

```
Console# clear counters ethernet g2
```

set interface active

The **set interface active** Privileged EXEC mode command reactivates an interface that was shutdown.

Syntax

set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}

Parameters

- *interface* — Valid Ethernet port. Elana
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shutdown by the system for some reason (e.g., **port security**).

Example

The following example reactivates interface 1.

```
Console# set interface active ethernet g1
```

show interfaces advertise

The **show interfaces advertise** Privileged EXEC mode command displays auto-negotiation data.

Syntax

show interfaces advertise [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.Elana
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays auto-negotiation information.

```
Console# show interfaces advertise


Port             Type             Neg              Operational
                                                   Link
                                                   Advertisement

----             -----------      -------          --------------
                                                   --------------
                                                   --

1                100M-Copper      Enabled          --

2                100M-Copper      Enabled          --

3                100M-Copper      Enabled          --

4                100M-Copper      Enabled          --

5                100M-Copper      Enabled          100f, 100h,
                                                   10f, 10h

6                100M-Copper      Enabled          --

7                100M-Copper      Enabled          --
```

```
8                 100M-Copper      Enabled          --

9                 100M-Copper      Enabled          --

10                100M-Copper      Enabled          --

11                100M-Copper      Enabled          --

12                100M-Copper      Enabled          --
```

show interfaces configuration

The **show interfaces configuration** Privileged EXEC mode command displays the configuration for all configured interfaces.

Syntax

show interfaces configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.Elana
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of all configured interfaces:

```
Console# show interfaces configuration


Port   Type   Dupl   Spee   Neg    Flow   Admi   Back   Mdix
              ex     d             Ctrl   n      Pres   Mode
                                          Stat   sure
                                          e
```

```
----   ----   ----   ----   ----   ----   ----   ----   ----
       ----   --     -      ---           -      ----
       ---

1      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

2      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

3      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

4      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

5      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

6      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

7      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

8      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

9      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

10     100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

11     100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per
```

show interfaces status

The s**how interfaces status** Privileged EXEC mode command displays the status of all configured interfaces.

Syntax

show interfaces status [**ethernet** *interface*| **port-channe**l *port-channel-number* |]

Parameters

- *interface* — A valid Ethernet port. Elana
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status of all configured interfaces.

```
Console# show interfaces status


Port   Type   Dupl   Spee   Neg    Flow   Link   Back   Mdix
              ex     d             Ctrl   Stat   Pres   Mode
                                          e      sure

----   ----   ----   ----   ----   ----   ----   ----   ----
       ----   --     -      ---           -      ----
       ---

1      100M   --     --     --     --     Down   --     --
       -Cop
       per

2      100M   --     --     --     --     Down   --     --
       -Cop
       per

3      100M   --     --     --     --     Down   --     --
       -Cop
       per
```

```
4      100M   --     --     --     --     Down   --     --
       -Cop
       per

5      100M   Full   100    Enab   Off    Up     Disa   Auto
       -Cop                 led                  bled
       per

6      100M   --     --     --     --     Down   --     --
       -Cop
       per

7      100M   --     --     --     --     Down   --     --
       -Cop
       per

8      100M   --     --     --     --     Down   --     --
       -Cop
       per

9      100M   --     --     --     --     Down   --     --
       -Cop
       per

10     100M   --     --     --     --     Down   --     --
       -Cop
       per

11     100M   --     --     --     --     Down   --     --
       -Cop
       per

12     100M   --     --     --     --     Down   --     --
       -Cop
       per
```

show interfaces description

The **show interfaces description** Privileged EXEC mode command displays the description for all configured interfaces.

Syntax

show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: unit/port)
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays descriptions of configured interfaces.

```
Console# show interfaces description


Port                                  Description
----                                  -----------
g1                                    lab
g2
g3
g4
g5
g6
ch1
ch2
```

show interfaces counters

The **show interfaces counters** Privileged EXEC mode command displays traffic seen by the physical interface.

Syntax

show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. Elana
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays traffic seen by the physical interface.

```
Console# show interfaces counters


Port         InOctets     InUcastPkts   InMcastPkts   InBcastPkts
----         --------     -----------   -----------   -----------
g1           183892       0             0             0
g1           0            0             0             0
g1           123899       0             0             0


Port         OutOctets    OutUcastPkt   OutMcastPkt   OutBcastPkt
                          s             s             s
-----        ----------   -----------   -----------   -----------
                          -             -             -
g1           9188         0             0             0
g1           0            0             0             0
g1           8789         0             0             0


Ch           InOctets     InUcastPkts   InMcastPkts   InBcastPkts
---          --------     ----------    -----------   -----------
1            27889        0             0             0
```

```
Ch             OutOctets     OutUcastPkt   OutMcastPkt   OutBcastPkt
                             s             s             s

---            ---------     -----------   -----------   -----------
                             -             -             -

1              23739         0             0             0
```

The following table describes the fields shown in the display.

```
Console# show interfaces counters ethernet 1


Port           InOctets      InUcastPkts   InMcastPkts   InBcastPkts

------         -----------   -----------   -----------   -----------
                             ---

g1             183892        0             0             0


Port           OutOctets     OutUcastPkt   OutMcastPkt   OutBcastPkt
                             s             s             s

------         -----------   -----------   -----------   -----------
                             ---           -             -

g1             9188          0             0             0


FCS Errors: 0

Single Collision Frames: 0

Late Collisions: 0

Excessive Collisions: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display.

Field	**Description**
InOctets	Counted received octets.
InUcastPkts	Counted received unicast packets.
InMcastPkts	Counted received multicast packets.

Field	Description
InBcastPkts	Counted received broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted unicast packets.
OutMcastPkts	Counted transmitted multicast packets.
OutBcastPkts	Counted transmitted broadcast packets.
FCS Errors	Counted received frames that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Number of excessive collisions received on the selected interface.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counted frames for which reception fails due to an internal MAC sublayer received error.
Received Pause Frames	Counted MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

port storm-control include-multicast (GC)

The **port storm-control include-multicast** Interface Configuration mode command enables counting multicast packets in the **port storm-control broadcast rate** command. To disable counting multicast packets, use the **no** form of this command.

Syntax

port storm-control include-multicast

no port storm-control include-multicast

Default Configuration

Multicast packets are not counted.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

To control multicasts storms, use the **port storm-control broadcast enable** and **port storm-control broadcast rate** commands.

Example

The following example enables counting multicast packets.

```
Console# configure
Console(config-if)# port storm-control include-multicast
Console(config-if)# port storm-control iinclude-multicast
unknown-unicast
```

port storm-control include-multicast (IC)

The **port storm-control include-multicast Interface** Configuration (Ethernet) mode command counts multicast packets in broadcast storm control. To disable counting multicast packets, use the **no** form of this command.

Syntax

port storm-control include-multicast [unknown-unicast]

no port storm-control include-multicast

Parameters

- **unknown-unicast** — Specifies also counting unknown unicast packets.

Default Configuration

Multicast packets are not counted.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables counting broadcast and multicast packets on Ethernet port 2.

```
Console(config)# interface ethernet 2
Console(config-if)# port storm-control include-multicast
unknown-unicast
```

port storm-control broadcast enable

The **port storm-control broadcast enable** Interface Configuration (Ethernet) mode command enables broadcast storm control. To disable broadcast storm control, use the **no** form of this command.

Syntax

port storm-control broadcast enable

no port storm-control broadcast enable

Default Configuration

Broadcast storm control is disabled.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

Use the **port storm-control broadcast rat**e Interface Configuration (Ethernet) mode command, to set the maximum allowable broadcast rate.

Use the **port storm-control include-multicast** Global Configuration mode command to enable counting multicast packets in the storm control calculation.

Example

The following example enables broadcast storm control on port 1 of a device.

```
Console(config)# interface ethernet 1
Console(config-if)# port storm-control broadcast enable
```

port storm-control broadcast rate

The **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command configures the maximum broadcast rate. To restore the default configuration, use the **no** form of this command.

Syntax

port storm-control broadcast rate rate

no port storm-control broadcast rate

Parameters

- *rate* — Maximum kilobits per second of broadcast and multicast traffic on a port. (Range of 3500-1000000)

Default Configuration

The default storm control broadcast rate is 3500 Kbits/Sec.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **port storm-control broadcast enable** Interface Configuration mode command to enable broadcast storm control.

Example

The following example configures a port storm-control broadcast rate 4000 on port g2.

```
(config)# interface ethernet g2
Console(config-if)# port storm-control broadcast rate 4000
```

show ports storm-control

The **show ports storm-control** Privileged EXEC mode command displays the storm control configuration.

Syntax

show ports storm-control [*interface*]

Parameters

- *interface* — A valid Ethernet port. Elana

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the storm control configuration.

```
Console# show ports storm-control


Port             State            Rate             Included
                                  [Kbits/Sec]

----             -----            --------------   --------
                                  --

g1               Disabled         3500             Broadcast

g2               Disabled         3500             Broadcast

g3               Disabled         3500             Broadcast

g4               Disabled         3500             Broadcast

g5               Disabled         3500             Broadcast

g6               Disabled         3500             Broadcast
```

6 LINE COMMANDS

line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

line {**console** | **telnet** | **ssh**}

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet
Console(config-line)#
```

speed

The **speed** Line Configuration mode command sets the line baud rate.

Syntax

speed *bps*

Parameters

- *bps* — Baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.

Default Configuration

The default speed is 19200 bps.

Command Mode

Line Configuration (console) mode

User Guidelines

This command is available only on the line console.

The configured speed is applied when Autobaud is disabled. This configuration applies only to the current session.

Example

The following example configures the line baud rate.

```
Console(config)# line console
Console(config-line)# speed 115200
```

autobaud

The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). To disable automatic baud rate detection, use the **no** form of the command.

Syntax

autobaud

no autobaud

Default Configuration

Autobaud is disabled.

Command Mode

Line Configuration (console) mode

User Guidelines

This command is available only on the line console.

To start communication using Autobaud , press <**Enter**> twice. This configuration applies only to the current session.

Example

The following example enables autobaud.l

```
Console(config)# line console
Console(config-line)# autobaud
```

exec-timeout

The **exec-timeout** Line Configuration mode command sets the interval that the system waits until user input is detected. To restore the default configuration, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters

- *minutes* — Specifies the number of minutes for the timeout. (Range: 0-65535)
- *seconds* — Specifies additional time intervals in seconds. (Range: 0-59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

To specify no timeout, enter the exec-timeout 0 command.

Example

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console(config)# line console
Console(config-line)# exec-timeout 20
```

history

The **history** Line Configuration mode command enables the command history function. To disable the command history function, use the **no** form of this command.

Syntax

history

no history

Default Configuration

The command history function is enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables the command history function for a specified line. To enable or disable the command history function for the current terminal session, use the **terminal history** user EXEC mode command.

Example

The following example enables the command history function for Telnet.

```
Console(config)# line telnet
Console(config-line)# history
```

history size

The **history size** Line Configuration mode command configures the command history buffer size for a particular line. To reset the command history buffer size to the default configuration, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

Parameters

- *number-of-commands*—Number of commands that the system records in its history buffer. (Range: 10-200)

Default Configuration

The default history buffer size is 10.

Command Mode

Line Configuration mode

User Guidelines

This command configures the command history buffer size for a particular line. To configure the command history buffer size for the current terminal session, use the **terminal history size** User EXEC mode command.

Example

The following example changes the command history buffer size to 100 entries for a particular line.

```
Console(config)# line telnet
Console(config-line)# history size 100
```

terminal history

The **terminal history** User EXEC mode command enables the command history function for the current terminal session. To disable the command history function, use the **no** form of this command.

Syntax

terminal history

no terminal history

Default Configuration

The default configuration for all terminal sessions is defined by the **history** line configuration command.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables the command history function for the current terminal session.

```
Console> terminal no history
```

terminal history size

The **terminal history size** User EXEC mode command configures the command history buffer size for the current terminal session. To reset the command history buffer size to the default setting, use the **no** form of this command.

Syntax

terminal history size *number-of-commands*

no terminal history size

Parameters

- *number-of-commands* — Specifies the number of commands the system may record in its command history buffer. (Range: 10-200)

Default Configuration

The default command history buffer size is 10.

Command Mode

User EXEC mode

User Guidelines

The **terminal history size** user EXEC command configures the size of the command history buffer for the current terminal session. To change the default size of the command history buffer, use the **history** line configuration command.

The maximum number of commands in all buffers is 256.

Example

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```

show line

The **show line** Privileged EXEC mode command displays line parameters.

Syntax

show line [console | telnet | ssh]

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

If the line is not specified, the default value is console.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the line configuration.

```
Console# show line


Console configuration:
                                  Interactive timeout: Disabled
                                  History: 10
                                  Baudrate: 9600
                                  Databits: 8
                                  Parity: none

                                  Stopbits: 1


Telnet configuration:

                                  Interactive timeout: 10 minutes
                                  10 seconds

                                  History: 10


SSH configuration:

                                  Interactive timeout: 10 minutes
                                  10 seconds

                                  History: 10
```

7 PHY DIAGNOSTICS COMMANDS

test copper-port tdr

The **test copper-port tdr** Privileged EXEC mode command uses Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test copper-port tdr *interface*

Parameters

- *interface* — A valid Ethernet port. Elana

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of cable for the TDR test is 120 meters.

Example

The following example results in a report on the cable attached to port g3.

```
Console# test copper-port tdr g3
Cable is open at 64 meters
Console# test copper-port tdr g3
Can’t perform this test on fiber ports
```

show copper-ports tdr

The **show copper-ports tdr** Privileged EXEC mode command displays information on the last Time Domain Reflectometry (TDR) test performed on copper ports.

Syntax

show copper-ports tdr [*interface*]

Parameters

- *interface* — A valid Ethernet port. Elana

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
Console# show copper-ports tdr
```

```
Port              Result            Length            Date
                                    [meters]

----              ------            --------------    ----
                                    -

g1                OK

g2                Short             50                13:32:00 23
                                                      July 2005

g3                Test has not been performed

g4                Open              64                13:32:00 23
                                                      July 2005

g5                Fiber             -                 -
```

show copper-ports cable-length

The **show copper-ports cable-length** Privileged EXEC mode command displays the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

Parameters

- *interface* — A valid Ethernet port. Elana

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working in 1000M mode.

Example

The following example displays the estimated copper cable length attached to all ports.

```
Console# show copper-ports cable-length


Port                              Length [meters]
----                              ---------------------
g1                                < 50
g2                                Copper not active
g3                                110-140
g1                                Fiber
```

show fiber-ports optical-transceiver

The **show fiber-ports optical-transceiver** Privileged EXEC mode command displays the optical transceiver diagnostics.

Syntax

s**how fiber-ports optical-transceiver** [*interface*] [*detailed*]

Parameters

- *interface* — A valid Ethernet port.Elana
- *detailed* — Detailed diagnostics.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To test optical transceivers, ensure a fiber link is present.

Example

The following example displays the optical transceiver diagnostics results.

```
Console# show fiber-ports optical-transceiver 21


                        Curre   Output
                        nt
Port    Temp    Volta   Power   Power   Input   LOS
                ge
----    ----    -----   -----   -----   -----   ---
                --      --      -
21      OK      OK      OK      OK      OK      No


Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power in milliWatts.
Input Power – Measured RX  received power in milliWatts.
LOS – Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

```
Console# show fiber-ports optical-transceiver 21 detailed
                              Current  Output
Port     Temp     Voltage  Power    Power    Input    LOS
         [C]      [Volt]   [mA]     [mWatt]  [mWatt]
----     ----     -------  -------  ------   -----    -------
21       34       3.35     8.43     2.72     7.71     No


Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power in milliWatts.
Input Power – Measured RX  received power in milliWatts.
LOS – Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

8 PORT CHANNEL COMMANDS

interface port-channel

The **interface port-channel** Global Configuration mode command enters the Global Configuration mode to configure a specific port-channel.

Syntax

i**nterface port-channel** *port-channel-number*

Parameters

- *port-channel-numbe*r — A valid port-channel number. (Range: 1-8)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Eight aggregated links can be defined with up to eight member ports per port-channel. The aggregated links’ valid IDs are 1-8.

Example

The following example enters the context of port-channel number 1.

```
Console(config)# interface port-channel 1
```

interface range port-channel

The **interface range port-channel** Global Configuration mode command enters the Global Configuration mode to configure multiple port-channels.

Syntax

interface range port-channel {*port-channel-range* | **all**}

Parameters

- *port-channel-range* — List of valid port-channels to add. Separate nonconsecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels. (Range: 1-8)
- **all** — All valid port-channels.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range.

Example

The following example groups port-channels 1, 2 and 6 to receive the same command.

```
Console(config)# interface range port-channel 1-2,6
```

channel-group

The **channel-group** Interface Configuration (Ethernet) mode command associates a port with a port-channel. To remove a port from a port-channel, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode** {**on** | **auto**}

no channel-group

Parameters

- *port-channel_number* — Specifies the number of the valid port-channel for the current port to join. (Range: 1-8)
- **on** — Forces the port to join a channel without an LACP operation.

- **auto** — Allows the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forces port 1 to join port-channel 1 without an LACP operation.

```
Console(config)# interface ethernet g1
Console(config-if)# channel-group 1 mode on
```

show interfaces port-channel

The **show interfaces port-channel** Privileged EXEC mode command displays port-channel information.

Syntax

show interfaces port-channel [*port-channel-number*]

Parameters

- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on all port-channels.

```
Console# show interfaces port-channel


Channel                         Ports

-------                         ------------------------------
                                --

1                               Active: g1, g2

2                               Active: g2, g7 Inactive: g1

3                               Active: g3, g8
```

9 QoS Commands

qos

The **qos** Global Configuration mode command enables quality of service (QoS) on the device. To disable QoS on the device, use the **no** form of this command.

Syntax

qos [basic | advanced]

no qos

Parameters

- **basic** — QoS basic mode.
- **advanced** — QoS advanced mode, which enables the full range of QoS configuration.

Default Configuration

The QoS basic mode is enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables QoS on the device.

```
Console(config)# qos basic
```

show qos

The **show qos** Privileged EXEC mode command displays the quality of service (QoS) mode for the device.

Syntax

show qos

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Example

The following example displays QoS attributes when QoS is enabled in basic mode on the device.

```
Console# show qos
Qos: basic
Basic trust: vpt
```

class-map

The **class-map** Global Configuration mode command creates or modifies a class map and enters the Class-map Configuration mode. To delete a class map, use the **no** form of this command.

Syntax

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name*

Parameters

- *class-map-name* — Specifies the name of the class map (Range: 0-32 characters).
- **match-all** — Checks that the packet matches all classification criteria in the class map match statement.

- **match-any** — Checks that the packet matches one or more classification criteria in the class map match statement.

Default Configuration

By default, the match-all parameter is selected.

Command Mode

Global Configuration mode

User Guidelines

The **class-map** Global Configuration mode command is used to define packet classification, marking and aggregate policing as part of a globally named service policy applied on a per-interface basis.

The Class-Map Configuration mode enables entering up to two **match** Class-map Configuration mode commands to configure the classification criteria for the specified class. If two **match** Class-map Configuration mode commands are entered, each should point to a different type of ACL (e.g., one to an IP ACL and one to a MAC ACL). Since packet classification is based on the order of the classification criteria, the order in which the **match** Class-Map Configuration mode commands are entered is important.

If there is more than one match statement in a **match-all** class map and the same classification field appears in the participating ACLs, an error message is generated.

Note:

A class map in match-all mode cannot be configured if it contains both an IP ACL and a MAC ACL with an ether type that is not 0x0800.

Example

The following example creates a class map called class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```

show class-map

The **show class-map** Privileged EXEC mode command displays all class maps.

Syntax

show class-map [*class-map-name*]

Parameters

- *class-map-name* — Specifies the name of the class map to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows the class map for class1.

```
Console# show class-map class1
Class Map match-any class1 (id4)
```

match

The **match** Class-map Configuration mode command defines the match criteria for classifying traffic. To delete the match criteria, use the **no** form of this command.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

- *acl-name* — Specifies the name of an IP or MAC ACL. (Range: 0-32 characters)

Default Configuration

No match criterion is supported.

Command Mode

Class-map Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the match criterion for classifying traffic as an access group called ‘enterprise’ in a class map called ‘class1’.

```
Console (config)# class-map class1
Console (config-cmap)# match access-group enterprise
```

policy-map

The **policy-map** Global Configuration mode command creates a policy map and enters the Policy-map Configuration mode. To delete a policy map, use the **no** form of this command.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

- *policy-map-name* — Specifies the name of the policy map (Range: 0-32 characters).

Command Mode

Global Configuration mode

User Guidelines

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created or modified.

Class policies in a policy map can only be defined if match criteria has already been defined for the classes. Use the class-map Global

Configuration and match **Class-map** Configuration commands to define the **match** criteria of a class.

Only one policy map per interface per direction is supported. A policy map can be applied to multiple interfaces and directions.

Example

The following example creates a policy map called ‘policy1’ and enters the Policy-map Configuration mode.

```
Console (config)# policy-map policy1
Console (config-pmap)#
```

class

The **class** Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. To remove a class map from the policy map, use the **no** form of this command.

Syntax

class *class-map-name* [**access-group** *acl-name*]

no class *class-map-name*

Parameters

- *class-map-name* — Specifies the name of an existing class map. If the class map does not exist, a new class map will be created under the specified name (Range: 0-32 characters).
- *acl-name* — Specifies the name of an IP or MAC ACL.

Default Configuration

No policy map is defined.

Command Mode

Policy-map Configuration mode

User Guidelines

Before modifying a policy for an existing class or creating a policy for a new class, use the **policy-map** Global Configuration mode command to specify the name of the policy map to which the policy belongs and to enter the Policy-map Configuration mode.

Use the **service-policy** (Ethernet, Port-channel) Interface Configuration mode command to attach a policy map to an interface. Use an existing class map to attach classification criteria to the specified policy map and use the **access-group** parameter to modify the classification criteria of the class map.

If this command is used to create a new class map, the name of an IP or MAC ACL must also be specified.

Example The following example defines a traffic classification called 'class1' with an access-group called 'enterprise'. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console (config-pmap)# class class1 access-group enterprise
```

show policy-map

The **show policy-map** Privileged EXEC mode command displays the policy maps.

Syntax

show policy-map [*policy-map-name* [*class-name*]]

Parameters

- *policy-map-name* — Specifies the name of the policy map to be displayed.
- *class-name* — Specifies the name of the class whose QoS policies are to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all policy maps.

```
Console# show policy-map
Policy Map policy1
  class class1
    set Ip dscp 7

Policy Map policy2
  class class 2
    police 96000 4800 exceed-action drop
  class class3
    police 124000 96000 exceed-action policed-dscp-transmit
```

trust cos-dscp

The **trust cos-dscp** Policy-map Class Configuration mode command configures the trust state. The trust state determines the source of the internal DSCP value used by Quality of Service (QoS). To restore the default configuration, use the **no** form of this command.

Syntax

trust cos-dscp

no trust cos-dscp

Default Configuration

The port is not in the trust mode.

If the port is in trust mode, the internal DSCP value is derived from the ingress packet.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Action serviced to a class, so that if an IP packet arrives, the queue is assigned per DSCP. If a non-IP packet arrives, the queue is assigned per CoS (VPT).

Example

The following example configures the trust state for a class called ‘class1’ in a policy map called ‘policy1’.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# trust cos dscp
```

set

The **set** Policy-map Class Configuration mode command sets new values in the IP packet.

Syntax

set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}

no set

Parameters

- *new-dscp* — Specifies a new DSCP value for the classified traffic. (Range: 0-63)
- *queue-id* — Specifies an explicit queue ID for setting the egress queue.
- *new-cos* — Specifies a new user priority for marking the packet. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

This command is mutually exclusive with the **trust** Policy-map Class Configuration command within the same policy map.

Policy maps that contain **set o**r **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an egress interface by using the **service-policy** (Ethernet, Port-channel) Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example sets the DSCP value in the packet to 56 for classes in policy map called ‘policy1’.

```
Console (config)# policy-map policy1
Console (config-pmap)# set dscp 56
```

police

The **police** Policy-map Class Configuration mode command defines the policer for classified traffic. To remove a policer, use the **no** form of this command.

Syntax

police *committed-rate-bps committed -burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no police

Parameters

- *committed-rate-bps* — Specifies the average traffic rate (CIR) in bits per second (bps).
- *committed -burst-byte* — Specifies normal burst size (CBS) in bytes.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bps, the packet is dropped. The class is called ‘class1’ and is in a policy map called ‘policy1’.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# police 124000 9600 exceed-action drop
```

service-policy

The **service-policy** Interface Configuration (Ethernet, port-Channel) mode command applies a policy map to the input of a particular interface. To detach a policy map from an interface, use the **no** form of this command.

Syntax

service-policy {**input** *policy-map-name*}

no service-policy {input}

Parameters

- *policy-map-name* — Specifies the name of the policy map to be applied to the input interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-Channel) mode

User Guidelines

Only one policy map per interface per direction is supported.

Example

The following example attaches a policy map called ‘policy1’ to the input interface.

```
Console(config-if)# service-policy input policy1
```

qos aggregate-policer

The **qos aggregate-policer** Global Configuration mode command defines the policer parameters that can be applied to multiple traffic classes within the same policy map. To remove an existing aggregate policer, use the **no** form of this command.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-bps excess-burst-byte* **exceed-action** {**drop | policed-dscp-transmit**}

no qos aggregate-policer

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer.
- *committed-rate-bps* — Specifies the average traffic rate (CIR) in bits per second (bps).
- *excess-burst-byte* — Specifies the normal burst size (CBS) in bytes.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked.

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

Policers that contain **set** or **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an output interface.

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device; traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps.

This policer can also be used in Cascade police to make a cascade policer.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration command must first be used to delete the aggregate policer from all policy maps.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines the parameters of a policer called 'policer1' that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bps, the packet is dropped.

```
Console (config)# qos aggregate-policer policer1 124000 96000
exceed-action drop
```

show qos aggregate-policer

The **show qos aggregate-policer** Privileged EXEC mode command displays the aggregate policer parameter.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines.

Example

The following example displays the parameters of the aggregate policer called ‘policer1’.

```
Console# show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

police aggregate

The **police aggregate** Policy-map Class Configuration mode command applies an aggregate policer to multiple classes within the same policy map. To remove an existing aggregate policer from a policy map, use the **no** form of this command.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Parameters ■

- *aggregate-policer-name* — Specifies the name of the aggregate policer.

·Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps or interfaces.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example applies the aggregate policer called ‘policer’1 to a class called ‘class1’ in policy map called ‘policy1’.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```

wrr-queue cos-map

The **wrr-queue cos-map** Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. To restore the default configuration, use the **no** form of this command.

Syntax

wrr-queue cos-map *queue-id cos1...cos8*

no wrr-queue cos-map [*queue-id*]

Parameters

- *queue-id* — Specifies the queue number to which the CoS values are mapped.
- *cos1...cos8* — Specifies CoS values to be mapped to a specific queue. (Range: 0-7)

Default Configuration

CoS values are mapped to 8 queues as follows:

Cos0 is mapped to queue 3.

Cos1 is mapped to queue 1.

Cos2 is mapped to queue 2.

Cos3 is mapped to queue 4.

Cos4 is mapped to queue 5.

Cos5 is mapped to queue 6.

Cos6 is mapped to queue 7.

Cos7 is mapped to queue 8.

Command Mode

Global Configuration mode

User Guidelines

This command can be used to distribute traffic into different queues, where each queue is configured with different Weighted Round Robin (WRR) and Weighted Random Early Detection (WRED) parameters.

It is recommended to specifically map a single VPT to a queue, rather than mapping multiple VPTs to a single queue. Use the **priority-queue out** Interface Configuration (Ethernet, Port-channel) mode command to enable expedite queues.

Example

The following example maps CoS 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

wrr-queue bandwidth

The **wrr-queue-bandwith** Interface Configuration (Ethernet, port-channel) mode command assigns weights to each Weighted Round Robin (WRR) queue. The weight ratio determines the frequency by which the packet scheduler dequeues packets from each queue. To restore the default configuration, use the **no** form of this command.

Syntax

wrr-queue bandwidth *weight1 weight2 ... weight_n*

no wrr-queue bandwidth

Parameters

- *weight1 weight2 ... weight_n* — Sets the ratio of the bandwidth assigned by the WRR packet scheduler for the packet queues. Separate each value by a space. (Range: 6-255)

Default Configuration

The default WRR weight ratio is one-eighth of the sum of all queue weights (each weight is set to 6).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Use the **priority-queue out num-of-queues** Global Configuration mode command to configure a queue as WRR or Strict Priority. Use this command to define a WRR weight per interface.

The weight ratio for each queue is defined by the queue weight divided by the sum of all queue weights (i.e., the normalized weight). This sets the bandwidth allocation for each queue.

A queue can be assigned a WRR weight of 0, in which case no bandwidth is allocated to the queue and the shared bandwidth is divided among the remaining queues.

All eight queues participate in the WRR, excluding the queues that are assigned as expedite queues. The weights of the expedite queues are ignored in the ratio calculation.

An expedite queue is a priority queue, and it is serviced before the other queues are serviced. Use the **priority-queue out** Interface Configuration (Ethernet, port-channel) mode command to enable expedite queues.

Example

The following example assigns a weight of 6 to each of the 8 WRR queues.

```
Console(config-if)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

priority-queue out num-of-queues

The **priority-queue out num-of-queues** Global Configuration mode command configures the number of expedite queues. To restore the default configuration, use the **no f**orm of this command.

Syntax

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Parameters

- *number-of-queues* — Specifies the number of expedite queues. Expedite queues have higher indexes. (Range: 0-4)

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

Configuring the number of expedite queues affects the Weighted Round Robin (WRR) weight ratio because fewer queues participate in the WRR.

Example

The following example configures the number of expedite queues as 0.

```
Console(config)# priority-queue out num-of-queues 0
```

traffic-shape

The **traffic-shape** Interface Configuration (Ethernet, port-channel) mode command configures the shaper of the egress port/queue. To disable the shaper, use the **no** form of this command.

Syntax

traffic-shape {*committed-rate committed-burst*}

no traffic-shape

Parameters

- *committed-rate* — Specifies the average traffic rate (CIR) in kilobits per second (kbps).
- (Range: 64 kbps-1000000)
- *excess-burst* — Specifies the excess burst size (CBS) in bytes.

Default Configuration

No shape is defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command activates the shaper on a specified egress port or egress queue.

To activate the shaper on an egress port, enter the Interface Configuration mode and specify the port number. The CIR and the CBS will be applied to the specified port.

Example

The following example sets a shaper on Ethernet port g5 when the average traffic rate exceeds 124 kbps or the normal burst size exceeds 10,000 bytes.

```
Console(config)# interface ethernet g5
Console(config-if) traffic-shape 124 10000
```

rate-limit interface configuration

The **rate-limit interface configuration** command mode limits the rate of the incoming traffic. The **no** form of this command is used to disable rate limit.

Syntax r

rate-limit kbps

no rate-limit

Parameters •

- *kbps — Maximum of kilobits per second of ingress traffic on a port. (Range: 1 - 1000000)*

Default Configuration

1000 Kbits/Sec

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command can be enabled on a specific port only if the port storm-control broadcast enable interface configuration command is not enabled on that port.

Examples

The following example limits the rate of the incoming traffic to 62.

```
Console(config-ip)# rate-limit 62
```

show qos interface

The **show qos interface** Privileged EXEC mode command displays Quality of Service (QoS) information on the interface.

Syntax

show qos interface [**ethernet** *interface-number* | **port-channel** *number* | *port-channel number]* [**queueing** | **policers** | **shapers**]

Parameters

- *interface-number* — Valid Ethernet port number.
- *number* — Valid port-channel number.
- **queuing** — Displays the queue strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers** — Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **shapers** — Displays all the policers configured for this interface, their setting and the number of policers currently unused.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

If no keyword is specified, port QoS mode (for example., DSCP trusted, CoS trusted, untrusted), default CoS value, DSCP-to-DSCP-mutation map attached to the port, and policy map attached to the interface are displayed.

If no interface is specified, QoS information about all interfaces is displayed.

Example

The following example displays the buffer settings for queues on Ethernet port 1.

```
Console# show qos interface ether-
net g1 buffers

Ethernet g1

Notify Q
depth


qi   Si
d    ze

1    12
     5

2    12
     5

3    12
     5

4    12
     5

5    12
     5

6    12
     5

7    12
     5

8    12
     5


qi                                         Threshold
d

1                                          10
                                           0

2                                          10
                                           0

3                                          10
                                           0
```

4								100		
5								N/A		
6								N/A		
7								N/A		
8								N/A		

qid	Min DP0	Max DP0	Prob DP0	Min DP1	Max DP1	Prob DP1	Min DP2	Max DP2	Prob DP2	Weight
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	50	60	13	65	80	6	85	95	4	2
6	50	60	13	65	80	6	85	95	4	2
7	50	60	13	65	80	6	85	95	4	2
8	50	60	13	65	80	6	85	95	4	2

qos map policed-dscp

The **qos map policed-dscp** Global Configuration mode command modifies the policed-DSCP map for remarking purposes. To restore the default map, use the **no** form of this command.

Syntax

qos map policed-dscp *dscp-list* **to** *dscp-mark-down*

no qos map policed-dscp

Parameters

- *dscp- list* — Specifies up to 8 DSCP values separated by a space. (Range: 0-63)
- *dscp-mark-down* — Specifies the DSCP value to mark down. (Range: 0-63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

DSCP values 3,11,19… cannot be remapped to other values.

Example

The following example marks down incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3 was not configured.
```

qos map dscp-queue

The **qos map dscp-queue** Global Configuration mode command modifies the DSCP to CoS map. To restore the default map, use the **no** form of this command.

Syntax

qos map dscp-queue *dscp-list* **to** *queue-id*

no qos map dscp-queue

Parameters

- *dscp-list* — Specifies up to 8 DSCP values separated by a space. (Range: 0 - 63)
- *queue-id* — Specifies the queue number to which the DSCP values are mapped.

Default Configuration

The following table describes the default map.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```

qos trust (Global)

The **qos trust** Global Configuration mode command configures the system to the basic mode and trust state. To return to the untrusted state, use the **no** form of this command.

Syntax

qos trust {cos | dscp}

no qos trust

Parameters

- **cos** — Indicates that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp** — Indicates that ingress packets are classified with packet DSCP values.

Default Configuration

CoS is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every device in the domain.

A switch port on an inter-QoS domain boundary can be configured to the DSCP trust state, and, if the DSCP values are different between the QoS domains, the DSCP to DSCP mutation map can be applied.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured as trust DSCP, traffic is mapped to a queue according to the DSCP-queue map.

Example

The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

qos trust (Interface)

The **qos trust** Interface Configuration (Ethernet, port-channel) mode command enables each port trust state while the system is in the basic QoS mode. To disable the trust state on each port, use the **no** form of this command.

Syntax

qos trust

no qos trust

Default Configuration

qos trust is enabled on each port when the system is in basic mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port 15 to the default trust state.

```
Console(config)# interface ethernet 15
Console(config-if) qos trust
```

qos cos

The **qos cos** Interface Configuration (Ethernet, port-channel) mode command defines the default CoS value of a port. To restore the default configuration, use the **no** form of this command.

Syntax

qos cos *default-cos*

no qos cos

Parameters ■

- *default-cos* — Specifies the default CoS value of the port. (Range: 0-7)

Default Configuration

Default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If the port is trusted, the default CoS value of the port is used to assign a CoS value to all untagged packets entering the port.

Example

The following example configures port g15 default CoS value to 3.

```
Console(config)# interface ethernet g15
Console(config-if) qos cos 3
```

qos dscp-mutation

The **qos dscp-mutation** Global Configuration mode command applies the DSCP Mutation map to a system DSCP trusted port. To restore the trust state with no DSCP mutation, use the **no** form of this command.

Syntax

qos dscp-mutation

no qos dscp-mutation

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

The DSCP to DSCP mutation map is applied to a port at the boundary of a Quality of Service (QoS) administrative domain.

If two QoS domains have different DSCP definitions, use the DSCP to DSCP mutation map to match one set of DSCP values with the DSCP values of another domain.

Apply the DSCP to DSCP mutation map only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports.

If the DSCP to DSCP mutation map is applied to an untrusted port, class of service (CoS) or IP-precedence trusted port, this command has no immediate effect until the port becomes DSCP-trusted.

Example

The following example applies the DSCP Mutation Map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```

qos map dscp-mutation

The **qos map dscp-mutation** Global Configuration mode command modifies the DSCP to DSCP mutation map. To restore the default DSCP to DSCP mutation map, use the **no** form of this command.

Syntax

qos map dscp-mutation *in-dscp* **to** *out-dscp*

no qos map dscp-mutation

Parameters

- *in-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)
- *out-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

This is the only map that is not globally configured. it is possible to have several maps and assign each one to different ports.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

security-suite enable

The **security-suite enable** Global Configuration mode command enables the security suite feature. Use the **no** form of this command to disable the security suite feature.

Syntax

security-suite enable global-rules-only

no security-suite enable

Parameters

- **global-rules-only** — Specifies that all the security suites commands would be only global commands. This setting saves space in the Ternary Content Addressable Memory (TCAM).

Default Configuration

No protection is configured.

Command Mode

Global Configuration mode

User Guidelines

MAC ACLs should be removed before the security-suite is enabled. The rules can be reentered after the security-suite is enabled.

If ACLs or policy maps are assigned on ports, per interface security-suite rules cannot be enabled.

Example

The following example enables the security suite feature and specifies that all the security suites commands would be only global commands.

```
Console(config)# security-suite enable global-rules-only
```

security-suite dos protect

The **security-suite dos protect** Global Configuration mode command protects the system from specific well-known Denial Of Service attacks. Use the **no** form of this command to disable protection.

Syntax

security-suite dos protect {**add** *attack* | **remove** *attack*}

no security-suite dos protect

Parameters

- *attack* — Specify the attack type. See the usage guidelines for list of attacks.

Default Configuration

No protection is configured.

Command Mode

Global Configuration mode

User Guidelines

The following table describes a list of DoS attacks and the protection type:

Attack	**Keyword**	**Protection**
Stacheldraht Distribution DoS attack	stacheldraht	Discard TCP packets with source TCP port equal to 16660.
Invasor Trojan	invasor-trojan	Discard TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
Back Orifice Trojan	back-orifice-trojan	Discard UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

Example

The following example protects the system from the Invasor Trojan.

```
Console(config)# security-suite dos protect add
invasor-trojan
```

security-suite deny martian-addresses

The **security-suite deny martian-addresses** Global Configuration mode command denies packets containing reserved IP addresses. Use the **no** form of this command to permit those addresses.

Syntax

s**ecurity-suite deny martian-addresses** {**reserved** | **add** {*ip-address* {*mask* | *prefix-length*}} | **remove** {i*p-address {mask* | *prefix-length*}}

no security-suite deny martian-addresses

Parameters

- *ip-address* — Specify the packets to discard, with that IP address as the source IP address or the destination IP address.
- *mask* — Specifies the network mask of the IP address.
- *prefix-length* — Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).

- **reserved** — Specify to discard packets with source address or destination address in the block of the reserved IP addresses. See the usage guidelines for a list of reserved addresses.

Default Configuration

Martian addresses are allowed.

Command Mode

Global Configuration mode

User Guidelines

The following table describes the reserved addresses:

Address block	**Present use**
0.0.0.0/8 (except 0.0.0.0/32 as source address)	Addresses in this block refer to source hosts on "this" network.
127.0.0.0/8	This block is assigned for use as the Internet host loopback address.
192.0.2.0/24	This block is assigned as "TEST-NET" for use in documentation and example code.
224.0.0.0/4 as source	This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.
240.0.0.0/4 (except 255.255.255.255/32 as destination address)	This block, formerly known as the Class E address space, is reserved.

The following table describes some other Special IP addresses:

Address block	**Present use**
10.0.0.0/8	Private-Use Networks.
169.254.0.0/16	This is the "link local" block. It is allocated for communication between hosts on a single link. Hosts obtain these addresses by auto-configuration, such as when a DHCP server may not be found.
172.16.0.0/12	Private-Use Networks.
192.88.99.0/24	This block is allocated for use as 6to4 relay anycast addresses.

Address block	Present use
192.168.0.0/16	Private-Use Networks.
198.18.0.0/15	This block has been allocated for use in benchmark tests of network interconnect devices.

Example

The following example discard all packets with a source address or a destination address in the block of the reserved IP addresses.

```
Console(config)# security-suite deny martian-addresses
reserved add 127.0.0.0/8
```

10 CLOCK COMMANDS

clock set

The **clock set** Privileged EXEC mode command manually sets the system clock.

Syntax

clock set *hh:mm:ss day month year*

or

clock set *hh:mm:ss month day year*

Parameters

- *hh:mm:ss* — Current time in hours (military format), minutes, and seconds. (hh: 0-23, mm: 0-59, ss: 0-59)
- *day* — Current day (by date) in the month. (Range: 1-31)
- *month* — Current month using the first three letters by name. (Range: Jan, …, Dec)
- *year* — Current year. (Range: 2000-2097)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
Console# clock set 13:32:00 7 Mar 2005
```

clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use **no** form of this command to disable external time source.

Syntax

clock source {sntp}

no clock source

Parameters

- **sntp** — SNTP servers

Default Configuration

No external clock source

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an external time source for the system clock.

```
Console(config)# clock source sntp
```

clock timezone

The **clock timezone** Global Configuration mode command sets the time zone for display purposes. To set the time to the Coordinated Universal Time (UTC), use the **no** form of this command.

Syntax

clock timezone *hours-offset* [**minutes** *minutes-offset]* [**zone** *acronym*]

no clock timezone

Parameters

- *hours-offset* — Hours difference from UTC. (Range: –12 hours to +13 hours)
- minutes-offset — Minutes difference from UTC. (Range: 0-59)
- *acronym* — The acronym of the time zone. (Range: Up to 4 characters)

Default Configuration

Clock set to UTC.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

The following example sets the timezone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```

clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). To configure the software not to automatically switch to summer time, use the **no** form of this command.

Syntax

clock summer-time recurring {**usa | eu |** {*week day month hh:mm week day month hh:mm*}} [**offset** *offset]* [**zone** *acronym*]

clock summer-time date date month year hh:mm date month year hh:mm [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *month date year hh:mm month date year hh:mm* [**offset** *offset*] [**zone** *acronym*]

no clock summer-time recurring

Parameters

- **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
- **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa** — The summer time rules are the United States rules.
- **eu** — The summer time rules are the European Union rules.
- *week* — Week of the month. (Range: 1-5, **first**, **last**)
- *day* — Day of the week (Range: first three letters by name, like **sun**)
- *date* — Date of the month. (Range:1-31)
- *month* — Month. (Range: first three letters by name, like Jan)
- *year* — year - no abbreviation (Range: 2000-2097)
- *hh:mm* — Time in military format, in hours and minutes. (Range: hh: 0-23, mm:0-59)
- *offset* — Number of minutes to add during summer time. (Range: 1-1440)
- *acronym* — The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)

Default Configuration

Summer time is disabled.

offset — Default is 60 minutes.

acronym — If unspecified default to the timezone acronym.

If the timezone has not been defined, the default is UTC.

Command Mode

Global Configuration mode

User Guidelines

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rule for daylight savings time:

- Start: First Sunday in April
- End: Last Sunday in October
- Time: 2 am local time

EU rule for daylight savings time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00)

Example

The following example sets summer time starting on the first Sunday in April at 2 am and finishing on the last Sunday in October at 2 am.

```
Console(config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.

Syntax

sntp authentication-key number **md5** value

no sntp authentication-key number

Parameters

- *number* — Key number (Range: 1-4294967295)

- *value* — Key value (Range: 1-8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

User Guidelines

Multiple keys can be generated.

Example

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

sntp authenticate

The **sntp authenticate** Global Configuration mode command grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. To disable the feature, use the **no** form of this command.

Syntax

s**ntp authenticate**

no sntp authenticate

Default Configuration

No authentication

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both unicast and broadcast.

Example

The following example defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
```

sntp trusted-key

The **sntp trusted-key** Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the **no** form of this command.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Parameters

- *key-number* — Key number of authentication key to be trusted. (Range: 1-4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both received unicast and broadcast.

If there is at least 1 trusted key, then unauthenticated messages will be ignored.

Example

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
```

sntp client poll timer

The **sntp client poll timer** Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. To restoreTo restoreTo restore default configuration, use the **no** form of this command.

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

Parameters

- *seconds* — Polling interval in seconds. (Range: 60-86400)

Default Configuration

Polling interval is 1024 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the polling time for the SNTP client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables SNTP anycast client. To disable the SNTP anycast client, use the **no** form of this command.

Syntax

sntp anycast client enable

no sntp anycast client enable

Default Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example

The following example enables SNTP anycast clients.

```
console(config)# sntp anycast client enable
```

sntp client enable (Interface)

The **sntp client enable** Interface Configuration (Ethernet, port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive broadcast and anycast updates. To disable the SNTP client, use the **no** form of this command.

Syntax

sntp client enable

no sntp client enable

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration (Ethernet, port-channel, VLAN) mode

User Guidelines

Use the **sntp anycast client enable** Global Configuration mode command to enable anycast clients globally.

Example

The following example enables the SNTP client on Ethernet port g3.

```
Console(config)# interface ethernet g3
Console(config-if)# sntp client enable
```

sntp unicast client enable

The **sntp unicast client enable** Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers. To disable requesting and accepting SNTP traffic from servers, use the **no** form of this command.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Configuration

The SNTP unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```
Console(config)# sntp unicast client enable
```

sntp unicast client poll

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast servers. To disable the polling for SNTP client, use the **no** form of this command.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the s**ntp client poll timer** Global Configuration mode command.

Example

The following example enables polling for SNTP predefined unicast clients.

```
Console(config)# sntp unicast client poll
```

sntp server

The **sntp server** Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

sntp server {*ip-address* | *hostname*}[**poll**] [**key** *keyid*]

no sntp server *host*

Parameters

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enable polling.
- *keyid* — Authentication key to use when sending packets to this peer. (Range:1-4294967295)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

Use the **sntp unicast client enable** Global Configuration mode command to enable predefined unicast clients globally.

To enable polling you should also use the **sntp unicast client poll** Global Configuration mode command for global enabling.

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

show clock

The **show clock** Privileged EXEC mode command displays the time and date from the system clock.

Syntax

show clock [detail]

Parameters

- **detail** — Shows timezone and summertime configuration.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The symbol that precedes the show clock display indicates the following:

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but SNTP is not synchronized.

Example

The following example displays the time and date from the system clock.

```
Console# show clock
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP

Console# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP
Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

show sntp configuration

The **show sntp configuration** Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

Syntax

show sntp configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the current SNTP configuration of the device.

```
Console# show sntp configuration


Polling interval: 1024 seconds


MD5 Authentication keys: 8, 9
```

```
Authentication is required for synchronization.
Trusted Keys: 8, 9

Unicast Clients Polling: Enabled

Server                Polling                Encryption Key
-----------           -------                --------------
176.1.1.8             Enabled                9
176.1.8.179           Disabled               Disabled

Broadcast Clients: Enabled
Anycast Clients: Enabled
Broadcast Interfaces: g1, g3
```

show sntp status

The **show sntp status** Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

Syntax

show sntp status

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows the status of the SNTP.

```
Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast

Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)


Unicast servers:

Server     Status     Last response          Offset     Delay
                                             [mSec]     [mSec]

--------   -------    --------------------   ------     ------
---                   --------

176.1.1.   Up         19:58:22.289 PDT Feb   7.33       117.79
8                     19 2005

176.1.8.   Unknown    12:17.17.987 PDT Feb   8.98       189.19
179                   19 2005


Anycast server:

Server     Interfac   Status     Last       Offset     Delay
           e                     response

                                            [mSec]     [mSec]

--------   -------    -----      --------   ------     -----
-                                --------
                                 --------
                                 -----

176.1.11   VLAN 118   Up         9:53:21.   7.19       119.89
.8                               789 PDT
                                 Feb 19
                                 2005


Broadcas
t:

Interfac   IP                    Last response
e          Address

--------   --------              ----------------------------
-          -
```

g13	0.0.0.0	00:00:00.0 Feb 19 2005	
vlan 1	16.1.1.200	15:15:16.0 LLBG Feb 19 2006	

11 RMON COMMANDS

show rmon statistics

The **show rmon statistics** Privileged EXEC mode command displays RMON Ethernet statistics.

Syntax

show rmon statistics {**ethernet** *interface numbe*r | *port-channel port-channel-number*}

Parameters

- *interface number* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet statistics for Ethernet port g1.

```
Console# show rmon statistics ethernet 1


Port: 1
Octets: 878128                    Packets: 978
Broadcast: 7                      Multicast: 1
CRC Align Errors: 0               Collisions: 0
Undersize Pkts: 0                 Oversize Pkts: 0
Fragments: 0                      Jabbers: 0
64 Octets: 98                     65 to 127 Octets: 0
128 to 255 Octets: 0              256 to 511 Octets: 0
512 to 1023 Octets: 491           1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display.

Field	**Description**
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	The total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.

Field	Description
Oversize Pkts	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

rmon collection history

The **rmon collection history** Interface Configuration (Ethernet, port-channel) mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Parameters

- *index* — Specifies the statistics group index . (Range: 1-65535)
- *ownername* — Specifies the RMON statistics group owner name. (Range: 0-160 characters)
- *bucket-number* — Number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range:1-65535)
- *seconds* — Number of seconds in each polling cycle. (Range: 1-3600)

Default Configuration

RMON statistics group owner name is an empty string.

Number of buckets specified for the RMON collection history statistics group is 50.

Number of seconds in each polling cycle is 1800.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Cannot be configured for a range of interfaces (Range context).

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on Ethernet port g1 with index number 1 and a polling interval period of 2400 seconds.

```
Console(config)# interface ethernet g1
Console(config-if)# rmon collection history 1 interval 2400
```

show rmon collection history

The **show rmon collection history** Privileged EXEC mode command displays the requested RMON history group statistics.

Syntax

show rmon collection history [**ethernet** *interface* | *port-channel port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. Elana
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all RMON history group statistics.

```
Console# show rmon collection history


Index      Interfac   Interval   Requeste   Granted    Owner
           e                     d          Samples
                                 Samples

-----      --------   --------   --------   -------    -------
           -                     -

1          g1         30         50         50         CLI

2          g1         1800       50         50         Manager
```

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry

show rmon history

The **show rmon history** Privileged EXEC mode command displays RMON Ethernet history statistics.

Syntax

show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]

Parameters

- ***index*** — Specifies the requested set of samples. (Range: 1-65535)
- **throughput** — Indicates throughput counters.
- **errors** — Indicates error counters.
- **other** — Indicates drop and collision counters.
- *seconds* — Specifies the period of time in seconds. (Range: 1-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet history statistics for index 1.

```
Console# show rmon history 1 throughput


Sample Set: 1         Owner: CLI

Interface: g1         Interval: 1800

Requested samples:    Granted samples: 50
50


Maximum table size: 500
```

```
Time       Octets     Packets    Broadcas   Multicas   Util
                                 t          t

--------   --------   -------    --------   --------   -----
--------   -                     --         -
----

Jan 18     30359596   357568     3289       7287       19%
2005       2
21:57:00

Jan 18     28769630   275686     2789       5878       20%
2005       4
21:57:30


Console# show rmon history 1 errors


Sample Set: 1          Owner: Me

Interface: g1          Interval: 1800

Requested samples:     Granted samples: 50
50


Maximum table size: 500 (800 after reset)


Time       CRC        Undersiz   Oversize   Fragment   Jabbers
           Align      e                     s

--------   --------   --------   --------   --------   -------
--         -          -                     -

Jan 18     1          1          0          49         0
2005
21:57:00

Jan 18     1          1          0          27         0
2005
21:57:30


Console# show rmon history 1 other
```

```
Sample Set: 1         Owner: Me

Interface: g1         Interval: 1800

Requested samples:    Granted samples: 50
50


Maximum table size: 500


Time                  Dropped    Collisio
                                 ns

-------------------   --------   --------
-                                --

Jan 18 2005           3          0
21:57:00

Jan 18 2005           3          0
21:57:30
```

The following table describes significant fields shown in the example:

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Util	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Field	**Description**
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

rmon alarm

The **rmon alarm** Global Configuration mode command configures alarm conditions. To remove an alarm, use the **no** form of this command.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

Parameters

- *index* — Specifies the alarm index. (Range: 1-65535)
- *variable* — Specifies the object identifier of the variable to be sampled.
- *interval* — Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 0-2147483647)

- *rthreshold* — Specifies the rising threshold. (Range: 0-2147483647)
- *fthreshold* — Specifies the falling threshold. (Range: 0-2147483647)
- *revent* — Specifies the event index used when a rising threshold is crossed.(Range: 1-65535)
- *fevent* — Specifies the event index used when a falling threshold is crossed. (Range: 1-65535)
- *type* — Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. Possible values are **absolute** and **delta.**

  If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- direction — Specifies the alarm that may be sent when this entry is first set to valid. Possible values are **rising**, **rising-falling** and **falling**.

  If the first sample (after this entry becomes valid) is greater than or equal to rthreshold and direction is equal to **rising** or **rising-falling**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to fthreshold and direction is equal to **falling** or **rising-falling**, a single falling alarm is generated.
- *name* — Specifies the name of the person who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The type is **absolute**.

The startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the following alarm conditions:

- Alarm index — 1000
- Variable identifier — 3Com

- Sample interval — 360000 seconds
- Rising threshold — 1000000
- Falling threshold — 1000000
- Rising threshold event index — 10
- Falling threshold event index — 20

```
Console(config)# rmon alarm 1000 3Com 360000 1000000 1000000 10
20
```

show rmon alarm-table

The **show rmon alarm-table** Privileged EXEC mode command displays the alarms table.

Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the alarms table.

```
Console# show rmon alarm-table


Index                  OID                    Owner

-----                  --------------------   -------
                       --

1                      1.3.6.1.2.1.2.2.1.10   CLI
                       .1
```

```
2                      1.3.6.1.2.1.2.2.1.10  Manager
                       .1

3                      1.3.6.1.2.1.2.2.1.10  CLI
                       .9
```

The following table describes significant fields shown in the example:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon alarm

The **show rmon alarm** Privileged EXEC mode command displays alarm configuration.

Syntax

show rmon alarm *number*

Parameters

- *number* — Specifies the alarm index. (Range: 1-65535)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	**Description**
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is **delta**, this value is the difference between the samples at the beginning and end of the period. If the sample type is **absolute**, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.

Field	Description
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

rmon event

The **rmon event** Global Configuration mode command configures an event. To remove an event, use the no form of this command.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

Parameters

- *index* — Specifies the event index. (Range: 1-65535)
- *type* — Specifies the type of notification generated by the device about this event. Possible values: **none**, **log**, **trap**, l**og-trap**.
- **community** *text* — If the specified notification type is **trap**, an SNMP trap is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description** *text* — Specifies a comment describing this event. (Range: 0-127 characters)
- *name* — Specifies the name of the person who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

If **log** is specified as the notification type, an entry is made in the log table for each event. If **trap** is specified, an SNMP trap is sent to one or more management stations.

Example

The following example configures an event identified as index 10 and for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```

show rmon events

The **show rmon events** Privileged EXEC mode command displays the RMON event table.

Syntax

show rmon events

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON event table.

```
Console# show rmon events


Index       Descript    Type        Communit    Owner       Last
            ion                     y                       time
                                                            sent

-----       --------    --------    --------    -------     --------
            ------                  -                       --------
                                                            ----
```

```
1          Errors     Log                    CLI        Jan 18
                                                        2006
                                                        23:58:17

2          High       Log-Trap   device      Manager    Jan 18
           Broadcas                                     2006
           t                                            23:59:48
```

The following table describes significant fields shown in the example:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon log

The **show rmon log** Privileged EXEC mode command displays the RMON log table.

Syntax

show rmon log [*event*]

Parameters

- *event* — Specifies the event index. (Range: 0-65535)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON log table.

```
Console# show rmon log

Maximum table size: 500

Event                 Description           Time

-------               --------------        ---------

1                     Errors                Jan 18 2006 23:48:19

1                     Errors                Jan 18 2006 23:58:17

2                     High Broadcast        Jan 18 2006 23:59:48


Console# show rmon log

Maximum table size: 500 (800 after reset)

Event                 Description           Time

-------               --------------        ---------

1                     Errors                Jan 18 2006 23:48:19

1                     Errors                Jan 18 2006 23:58:17

2                     High Broadcast        Jan 18 2006 23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

rmon table-size

The **rmon table-size** Global Configuration mode command configures the maximum size of RMON tables. To return to the default configuration, use the **no f**orm of this command.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {history | log}

Parameters

- **history** *entries* — Maximum number of history table entries. (Range: 20 -32767)
- **log** *entries* — Maximum number of log table entries. (Range: 20-32767)

Default Configuration

History table size is 270.

Log table size is 200.

Command Mode

Global Configuration mode

User Guidelines

The configured table size taskes effect after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 100 entries.

```
Console(config)# rmon table-size history 100
```

12 IGMP SNOOPING COMMANDS

ip igmp snooping (Global)

The **ip igmp snooping** Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping.

```
Console(config)# ip igmp snooping
```

ip igmp snooping (Interface)

The **ip igmp snooping** Interface Configuration (VLAN) mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the no form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled .

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping
```

ip igmp snooping mrouter learn-pim-dvmrp

The **ip igmp snooping mrouter learn-pim-dvmrp** Interface Configuration (VLAN) mode command enables automatic learning of multicast device ports in the context of a specific VLAN. To remove automatic learning of multicast device ports, use the **no** form of this command.

Syntax

ip igmp snooping mrouter learn-pim-dvmrp

no ip igmp snooping mrouter learn-pim-dvmrp

Default Configuration

Automatic learning of multicast device ports is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Multicast device ports can be configured statically using the **bridge multicast forward-all** Interface Configuration (VLAN) mode command.

Example

The following example enables automatic learning of multicast device ports on VLAN 2.

```
Console(config) # interface vlan 2
Console(config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

ip igmp snooping host-time-out

The **ip igmp snooping host-time-out** Interface Configuration (VLAN) mode command configures the host-time-out. If an IGMP report for a multicast group was not received for a host-time-out period from a specific port, this port is deleted from the member list of that multicast group. To restore the default configuration, use the no form of this command.

Syntax

ip igmp snooping host-time-out time-out

no ip igmp snooping host-time-out

Parameters

- *time-out* — Specifies the host timeout in seconds. (Range: 1-2147483647)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

Example

The following example configures the host timeout to 300 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping host-time-out 300
```

ip igmp snooping mrouter-time-out

The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command configures the mrouter-time-out. The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command is used for setting the aging-out time after multicast device ports are automatically learned. To restore the default configuration, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out time-out

no ip igmp snooping mrouter-time-out

Parameters

- *time-out* — Specifies the Multicast device timeout in seconds (Range: 1-2147483647)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the multicast device timeout to 200 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter-time-out 200
```

ip igmp snooping leave-time-out

The **ip igmp snooping leave-time-out** Interface Configuration (VLAN) mode command configures the leave-time-out. If an IGMP report for a multicast group was not received for a leave-time-out period after an IGMP Leave was received from a specific port, this port is deleted from the member list of that multicast group.To restore the default configuration, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}

no ip igmp snooping leave-time-out

Parameters

- *time-out* — Specifies the leave-timeout in seconds for IGMP queries. (Range: 0-2147483647)
- **immediate-leave** — Indicates that the port should be immediately removed from the members list after receiving IGMP Leave.

Default Configuration

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP query.

Use immediate leave only where there is just one host connected to a port.

Example

The following example configures the host leave timeout to 60 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping leave-time-out 60
```

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** Privileged EXEC mode command displays information on dynamically learned multicast device interfaces.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

Parameters

- *vlan-id* — Specifies the VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays multicast device interfaces in VLAN 1000.

```
Console# show ip igmp snooping mrouter interface 1000


VLAN                              Ports

----                              -----

1000                              g1


Detected multicast devices that are forbidden statically:

VLAN                              Ports

----                              -----

1000                              g19
```

show ip igmp snooping interface

The **show ip igmp snooping interface** Privileged EXEC mode command displays IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays IGMP snooping information on VLAN 1000.

```
Console# show ip igmp snooping interface 4

IGMP Snooping is globaly disabled
IGMP Snooping is enabled on VLAN 4
IGMP host timeout is 260 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

show ip igmp snooping groups

The show **ip igmp snooping groups** Privileged EXEC mode command displays multicast groups learned by IGMP snooping.

Syntax

s**how ip igmp snooping groups** [**vlan** *vlan-id*] [**address** *ip-multicast-address*]

Parameters

- *vlan-id* — Specifies the VLAN number.
- *ip-multicast-address* — Specifies the IP multicast address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To see the full multicast address table (including static addresses) use the **show bridge multicast address-table** Privileged EXEC command.

Example

The following example shows IGMP snooping information on multicast groups.

```
Console# show ip igmp snooping groups


Vlan            IP Address       Querier         Ports

----            --------------   -------         ----------
                ---

1               224-239.130|2.   Yes             g1, g2
                2.3

19              224-239.130|2.   Yes             g9-11
                2.8


IGMP Reporters that are forbidden statically:

---------------------------------------------

Vlan            IP Address       Ports

----            --------------   -----
                ---

1               224-239.130|2.   g19
                2.3
```

13 LACP COMMANDS

lacp system-priority

The **lacp system-priority** Global Configuration mode command configures the system priority. To restore the default configuration, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

Parameters

- *value* — Specifies system priority value. (Range: 1-65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the system priority to 120.

```
Console(config)# lacp system-priority 120
```

lacp port-priority

The **lacp port-priority** Interface Configuration (Ethernet) mode command configures physical port priority. To return to the default configuration, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

- *value* — Specifies port priority. (Range: 1-65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the priority of Ethernet port g6 as 247.

```
Console(config)# interface ethernet g6
Console(config-if)# lacp port-priority 247
```

lacp timeout

The **lacp timeout** Interface Configuration (Ethernet) mode command assigns an administrative LACP timeout. To return to the default configuration, use the **no** form of this command.

Syntax

lacp timeout {**long** | **short**}

no lacp timeout

Parameters

- **long** — Specifies the long timeout value.
- **short** — Specifies the short timeout value.

Default Configuration

The default port timeout value is long.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns a long administrative LACP timeout to Ethernet port g6.

```
Console(config)# interface ethernet g6
Console(config-if)# lacp timeout long
```

show lacp ethernet

The **show lacp** ethernet Privileged EXEC mode command displays LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters | statistics** | **protocol-state**]

Parameters

- *interface* — Valid Ethernet port.Elana
- **parameters** — Link aggregation parameter information.
- **statistics** — Link aggregation statistics information.
- **protocol-state** — Link aggregation protocol-state information.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example display LACP information for Ethernet port 1.

```
Console# show lacp ethernet g1


1 LACP parameters:

                Actor

                                system           1
                                priority:

                                system mac       00:00:12:34:56
                                addr:            :78

                                port Admin       30
                                key:

                                port Oper key:   30

                                port Oper        21
                                number:

                                port Admin       1
                                priority:

                                port Oper        1
                                priority:

                                port Admin       LONG
                                timeout:

                                port Oper        LONG
                                timeout:

                                LACP Activity:   ACTIVE

                                Aggregation:     AGGREGATABLE

                                collecting:      FALSE

                                distributing:    FALSE

                                expired:         FALSE

                Partner

                                system           0
                                priority:

                                system mac       00:00:00:00:00
                                addr:            :00

                                port Admin       0
                                key:
                                port Oper key:   0

                                port Oper        0
                                number:

                                port Admin       0
                                priority:

                                port Oper        0
                                priority:

                                port Oper        LONG
                                timeout:

                                LACP Activity:   PASSIVE

                                Aggregation:     AGGREGATABLE

                                synchronizatio   FALSE
                                n:

                                collecting:      FALSE

                                distributing:    FALSE

                                expired:         FALSE


g1 LACP Statistics:

LACP PDUs sent:                                    2

LACP PDUs received:                                2


g1 LACP Protocol State:

                LACP State Machines:

                                Receive FSM:     Port Disabled
                                                 State

                                Mux FSM:         Detached State

                                Periodic Tx      No Periodic
                                FSM:             State

                Control Variables:

                                BEGIN:           FALSE

                                LACP_Enabled:    TRUE

                                Ready_N:         FALSE

                                Selected:        UNSELECTED
```

```
                             Port_moved:      FALSE
                             NNT:             FALSE
                             Port_enabled:    FALSE
                 Timer counters:
                             periodic tx      0
                             timer:
                             current while    0
                             timer:
                             wait while       0
                             timer:
```

show lacp port-channel

The **show lacp port-channel** Privileged EXEC mode command displays LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

Parameters

- *port_channel_number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays LACP information about port-channel 1.

```
Console# show lacp port-channel 1
Port-Channel ch1
```

```
Port Type Gigabit Ethernet

Attached Lag id:

Actor

                 System           1
                 Priority:

                 MAC Address:
                                  00:02:85:0E:1C
                                  :00

                 Admin Key:        1000

                 Oper Key:         1000


 Partner

                 System           0
                 Priority:

                 MAC Address:
                                  00:00:00:00:00
                                  :00

                 Oper Key:         14
```

14 POWER OVER ETHERNET COMMANDS

power inline

The **power inline** Interface Configuration mode command configures the administrative mode of the inline power on an interface.

Syntax

power inline {auto | never}

Parameters

- ***auto*** — Turns on the device discovery protocol and applies power to the device.
- **never** — Turns off the device discovery protocol and stops supplying power to the device.

Default Configuration

Auto

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example turns on the device discovery protocol on port 4.

```
Console(config)# interface ethernet 4
Console(config-if)# power inline auto
```

power inline powered-device

The **power inline powered-device** Interface Configuration mode command adds a description of the powered device type. Use the **no** form of this command to remove the description.

Syntax

power inline powered-device *pd-type*

no power inline powered-device

Parameters

- *pd-type* — Comment or a description to assist in recognising what is the type of the powered device attached to this interface. (Range: up to 24 characters)

Default Configuration

There is no default configuration for this command.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a description of the device connected to port 4 as ‘ip phone’.

```
Console(config)# interface ethernet 4
Console(config-if)# power inline powered-device ip phone
```

power inline priority

The **power inline priority** Interface Configuration mode command configures the priority of the interface from the point of view of inline power management. Use the **no** form of this command to restore defaults.

Syntax

power inline priority {critical | high | low}

no power inline priority

Parameters

- **critical** — The operation of the powered device is critical.
- **high** — The operation of the powered device is in high priority.
- **low** — The operation of the powered is in low priority.

Default Configuration

Low priority

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the priority of port 4 from the point of view of inline power management to ‘high’.

```
Console(config)# interface ethernet 4
Console(config-if)# power inline priority high
```

power inline usage-threshold

The **power inline usage-threshold** Global Configuration mode command configures the threshold for initiating inline power usage alarms. Use the **no** form of this command to restore defaults.

Syntax

power inline usage-threshold *percents*

no power inline usage-threshold

Parameters

- *percents* — Specifies the threshold in percents to compare to measured power. (Range: 1–99%)

Default Configuration

The default threshold is 95%.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command. Example

The following example configures the threshold for initiating inline power usage alarms to 90 percent.

```
Console(config)# power inline usage-threshold 90
```

power inline traps enable

The **power inline traps enable** Global Configuration mode command enable inline power traps. Use the **no** form of this command to disable traps.

Syntax

power inline traps enable

no power inline traps enable

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables inline power traps.

```
Console(config)# power inline traps enable
```

show power inline

The **show power inline** Privileged EXEC mode command displays information about the inline power.

Syntax

show power inline [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. Elana

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the inline power.

```
Console# show power inline



Unit     Power    Nominal  Consume  Usage    Thresho  Traps
                  Power    r Power           ld

----     -----    -----    -------  ------   -------  -----
                           --                --

1        On       400      0 Watts  (0%)     95       Disabl
                  Watts                               e


                  Admin                      Oper

Port     Powere   State    Status   Priorit  Class
         d                          y
         Device

----     ------   ------   ------   -------  ------
         ------            --       -        -
         ---
```

```
1                 Auto     Search   low      class0
                           ing

2                 Auto     Search   low      class0
                           ing

3                 Auto     Search   low      class0
                           ing




Console# show power inline ethernet 1


                  Admin                      Oper

Port     Powere   State    Priori            State    Class
         d                 ty
         Device

----     ------   ------   ------            ------   ------
         ------            --                -        --
         ------
         --

g1       IP       Auto     High              On       Class
         Phone                                        0
         Model
         A


Overload Counter: 1
Short Counter: 0
Denied Counter: 0
Absent Counter: 0
Invalid Signature Counter: 0
```

The following table describes the fields shown in the display:

Field	**Description**
Power	The inline power sourcing equipment operational status.
Nominal Power	The inline power sourcing equipment nominal power in Watts.
Consumed Power	Measured usage power in Watts.

Field	**Description**
Usage Threshold	The usage threshold expressed in percents for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	The Ethernet port number.
Powered device	A description of the powered device type.
Admin State	Indicates if the port is enabled to provide power. Admin State can be Auto or Never.
Priority	The priority of the port from the point of view of inline power management. Priority can be Critical, High or Low.
Oper State	Describes the inline power operational state of the port. Oper State can be On, Off, Test-Fail, Testing, Searching or Fault.
Classification	Power consumption classification of the powered device.
Overload Counter	Counts the number of overload conditions that has been detected.
Short Counter	Counts the number of short conditions that has been detected.
Denied Counter	Counts the number of times power has been denied.
Absent Counter	Counts the number of times power has been removed because powered device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a powered device was detected.

15 SPANNING-TREE COMMANDS

spanning-tree

The **spanning-tree** Global Configuration mode command enables spanning-tree functionality. To disable the spanning-tree functionality, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning-tree is enabled.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

spanning-tree mode

The **spanning-tree mode** Global Configuration mode command configures the spanning-tree protocol. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {**stp** | **rstp**| **mstp**} no spanning-tree mode

Parameters

- **stp** — Indicates that the Spanning Tree Protocol (STP) is enabled.
- **rstp** — Indicates that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp** — Indicates that the Multiple Spanning Tree Protocol (RSTP) is enabled.

Default Configuration

STP is enabled.

Command Modes

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP and uses STP when the neighbor device uses STP.

Example

The following example configures the spanning-tree protocol to RSTP.

```
console(config)# spanning-tree mode rstp
```

spanning-tree forward-time

The **spanning-tree forward-time** Global Configuration mode command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. To restore the default configuration, use the **no** form of this command.

Syntax

s**panning-tree forward-time** *seconds*

no spanning-tree forward-time

Parameters

- *seconds* — Time in seconds. (Range: 4-30)

Default Configuration

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be kept:

2*(Forward-Time - 1) >= Max-Age

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

spanning-tree hello-time

The **spanning-tree hello-time** Global Configuration mode command configures the spanning tree bridge hello time, which is how often the device broadcasts hello messages to other devices.To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Parameters

- *seconds* — Time in seconds. (Range: 1-10)

Default Configuration

The default hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

Command Modes

Global Configuration mode

User Guidelines

When configuring the hello time, the following relationship should be kept:

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures spanning tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

spanning-tree max-age

The **spanning-tree max-age** Global Configuration mode command configures the spanning tree bridge maximum age. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters

- *seconds* — Time in seconds. (Range: 6-40)

Default Configuration

The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

Command Modes

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be kept:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

spanning-tree priority

The **spanning-tree priority** Global Configuration mode command configures the spanning tree priority of the device. The priority value is used to determine which bridge is elected as the root bridge. To restore the default configuration, use the **no** form of this command.

Syntax

s**panning-tree priority** *priority*

no spanning-tree priority

Parameters

- *priority* — Priority of the bridge. (Range: 0-61440 in steps of 4096)

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Modes

Global Configuration mode

User Guidelines

The bridge with the lowest priority is elected as the root bridge.

Example

The following example configures spanning tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

spanning-tree disable

The **spanning-tree disable** Interface Configuration mode command disables spanning tree on a specific port. To enable spanning tree on a port, use the **no** form of this command.

Syntax

spanning-tree disable

no spanning-tree disable

Default Configuration

Spanning tree is enabled on all ports.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables spanning-tree on Ethernet port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree disable
```

spanning-tree cost

The **spanning-tree cost** Interface Configuration mode command configures the spanning tree path cost for a port. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

Parameters ■

- *cost* — Path cost of the port (Range: 1-200,000,000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4

Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The path cost method is configured using the **spanning-tree pathcost method** Global Configuration mode command.

Example

The following example configures the spanning-tree cost on Ethernet port g15 to 35000.

```
Console(config)# interface ethernet g15
Console(config-if)# spanning-tree cost 35000
```

spanning-tree port-priority

The **spanning-tree port-priority** Interface Configuration mode command configures port priority. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

- *priority* — The priority of the port. (Range: 0-240 in multiples of 16)

Default Configuration

The default port priority for IEEE Spanning TreeProtocol (STP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning priority on Ethernet port g15 to 96.

```
Console(config)# interface ethernet g15
Console(config-if)# spanning-tree port-priority 96
```

spanning-tree portfast

The **spanning-tree portfas**t Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup without waiting for the standard forward time delay. To disable PortFast mode, use the **no** form of this command.

Syntax

spanning-tree portfast [*auto*]

no spanning-tree portfast

Parameters

- **auto** — Specifies that the software waits for 3 seconds (With no BPDUs received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is disabled.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt device and network operations.

Example

The following example enables PortFast on Ethernet port g15.

```
Console(config)# interface ethernet g15
Console(config-if)# spanning-tree portfast
```

spanning-tree link-type

The **spanning-tree link-type** Interface Configuration mode command overrides the default link-type setting determined by the duplex mode of the port and enables Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree link-type {point-to-point | shared}

no spanning-tree spanning-tree link-type

Parameters

- **point-to-point** —Indicates that the port link type is point-to-point.
- **shared** — Indicates that the port link type is shared.

Default Configuration

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables shared spanning-tree on Ethernet port g15.

```
Console(config)# interface ethernet g15
Console(config-if)# spanning-tree link-type shared
```

spanning-tree pathcost method

The **spanning-tree pathcost method** Global Configuration mode command sets the default path cost method. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

Parameters

- *long* — Specifies port path costs with a range of 1-200,000,000 .
- *short* — Specifies port path costs with a range of 0-65,535.

Default Configuration

Short path cost method.

Command Mode

Global Configuration mode

User Guidelines

This command is only operational with the device in Interface mode.

This command applies to all spanning tree instances on the device.

The cost is set using the **spanning-tree cost** command.

Example

The following example sets the default path cost method to long.

```
Console(config)# spanning-tree pathcost method long
```

spanning-tree bpdu

The **spanning-tree bpdu** Global Configuration mode command defines BPDU handling when the spanning tree is disabled globally or on a single interface. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree bpdu {filtering | flooding}

no spanning-tree bpdu

Parameters

- **filtering** — Filter BPDU packets when the spanning tree is disabled on an interface.

- **flooding** — Flood BPDU packets when the spanning tree is disabled on an interface.

Default Configuration

The default setting is flooding.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines BPDU packet flooding when the spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```

clear spanning-tree detected-protocols

The **clear spanning-tree detected-protocols** Privileged EXEC mode command restarts the protocol migration process (forces renegotiation with neighboring devices) on all interfaces or on a specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number]*

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

This feature should be used only when working in RSTP or MSTP mode.

Example

The following example restarts the protocol migration process on Ethernet port g11.

```
Console# clear spanning-tree detected-protocols ethernet g11
```

spanning-tree mst priority

The **spanning-tree mst priority** Global Configuration mode command configures the device priority for the specified spanning-tree instance. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Parameters

- *instance -id*—ID of the spanning -tree instance (Range: 1-15).
- *priority*—Device priority for the specified spanning-tree instance (Range: 0-61440 in multiples of 4096).

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Mode

Global Configuration mode

User Guidelines

The device with the lowest priority is selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

spanning-tree mst max-hops

The **spanning-tree mst priority** Global Configuration mode command configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Parameters

- *hop-count*—Number of hops in an MST region before the BDPU is discarded .(Range: 1-40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

The **spanning-tree mst port-priority** Interface Configuration mode command configures port priority for the specified MST instance. To restore the default configuration, use the no form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters

- *instance-ID*—ID of the spanning tree instance. (Range: 1-15)
- *priority*—The port priority. (Range: 0-240 in multiples of 16)

Default Configuration

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the port priority of port g1 to 144.

```
Console(config)# interface ethernet g1
Console(config-if)# spanning-tree mst 1 port-priority 144
```

spanning-tree mst cost

The **spanning-tree mst cost** Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Parameters

- *instance-ID*—ID of the spanning -tree instance (Range: 1-16).
- *cost*—The port path cost. (Range: 1-200,000,000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	**Long**	**Short**
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4

Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the MSTP instance 1 path cost for Ethernet port 9 to 4.

```
Console(config) # interface ethernet 9
Console(config-if) # spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

The **spanning-tree mst configuration** Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

Example

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)#
```

instance (mst)

The **instance** MST Configuration mode command maps VLANS to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

Parameters

- *instance-ID*—ID of the MST instance (Range: 1-15).
- *vlan-range*—VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4094).

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
```

name (mst)

The **name** MST Configuration mode command defines the configuration name. To restore the default setting, use the **no** form of this command.

Syntax

name *string*

Parameters

- *string* — MST configuration name. The name is case-sensitive. (Range: 1-32 characters)

Default Configuration

The default name is the MAC address.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the configuration name as region1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # name region1
```

revision (mst)

The **revision MST** Configuration mode command defines the configuration revision number. To restore the default configuration, use the **no** form of this command.

Syntax

revision *value*

no revision

Parameters

- *value* — Configuration revision number (Range: 0-65535).

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

show (mst)

The **show** MST Configuration mode command displays the current or pending MST region configuration.

Syntax

show {current | pending}

Parameters

- **current**—Indicates the current region configuration.
- **pending**—Indicates the pending region configuration.

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

The pending MST region configuration takes effect only after exiting the MST Configuration mode.

Example

The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending

Pending MST configuration

Name: Region1

Revision: 1
```

```
Instance        Vlans Mapped    State
--------        ------------    -------
0               1-9,21-4094     Enabled
1               10-20           Enabled
```

exit (mst)

The **exit** MST Configuration mode command exits the MST Configuration mode, and applies all configuration changes.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example exits the MST Configuration mode and saves changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # exit
Console(config) #
```

abort (mst)

The **abort** MST Configuration mode command exits the MST Configuration mode without applying the configuration changes.

Syntax

abort

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example exits the MST Configuration mode without saving changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # abort
```

spanning-tree guard root

The **spanning-tree guard root** Interface Configuration (Ethernet, port-channel) mode command enables root guard on all spanning tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. To disable root guard on the interface, use the **no** form of this command.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Configuration

Root guard is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Root guard can be enabled when the device operates in STP, RSTP and MSTP.

When root guard is enabled, the port changes to the alternate state if spanning-tree calculations selects the port as the root port.

Example

The following example prevents Ethernet port g1 from being the root port of the device.

```
Console(config) # interface ethernet g1
Console(config-mst) # spanning-tree guard root
```

show spanning-tree

The **show spanning-tree** Privileged EXEC mode command displays spanning-tree configuration.

Syntax

show spanning-tree [**ethernet** *interface -number*| **port-channel** *port-channel-number*] [**instance** *instance-id*]

show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]

show spanning-tree mst-configuration

Parameters

- *interface* -number— A valid Ethernet port.
- *port-channel-number* — A valid port channel number.
- **detail** — Indicates detailed information.
- **active** — Indicates active ports only.
- **blockedports** — Indicates blocked ports only.
- **mst-configuration**— Indicates the MST configuration identifier.
- *instance-id*—Specifies ID of the spanning tree instance.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays spanning-tree information.

```
Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: short


CST     Prior           32768
Root    ity
ID

        Addre           00:01:42:97:e0:00
        ss

        Path            20000
        Cost

        Root            1 (1)
        Port


Bridg   Prior           36864
e ID    ity

        Addre           00:02:4b:29:7a:00
        ss

        Hello Time 2    Max Age 20 sec  Forward Delay 15 sec
        sec

        Max             20
        hops

Interfaces

Name    State   Prio.   Cost    Sts     Role    PortF   Type
                Nbr                             ast

----    -----   -----   -----   ---     ----    -----   -----
        --      ---                             ---     -----

g1      Enabl   128.1   20000   FWD     Root    No      P2p
        ed                                              bound
                                                        (RSTP
                                                        )
```

```
g2      Enabl   128.2   20000   FWD     Desg    No      Share
        ed                                              d
                                                        (STP)

g3      Disab   128.3   20000   -       -       -       -
        led

g4      Enabl   128.4   20000   BLK     ALTN    No      Share
        ed                                              d
                                                        (STP)

g5      Enabl   128.5   20000   DIS     -       -       -
        ed


Console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: long


Root    Prior           36864
ID      ity

        Addre           00:02:4b:29:7a:00
        ss

        This switch is the root.

        Hello Time 2    Max Age 20 sec  Forward Delay 15 sec
        sec


Interfaces

Name    State   Prio.   Cost    Sts     Role    PortF   Type
                Nbr                             ast

----    -----   -----   -----   ---     ----    -----   -----
        --      ---                             ---     -----

g1      Enabl   128.1   20000   FWD     Desg    No      P2p
        ed                                              (RSTP
                                                        )

g2      Enabl   128.2   20000   FWD     Desg    No      Share
        ed                                              d
                                                        (STP)
```

```
g3       Disab    128.3    20000    -        -        -        -
         led
g4       Enabl    128.4    20000    FWD      Desg     No       Share
         ed                                                    d
                                                               (STP)
g5       Enabl    128.5    20000    DIS      -        -        -
         ed


Console# show spanning-tree


Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long


Root     Prior             N/A
ID       ity
         Addre             N/A
         ss
         Path              N/A
         Cost
         Root              N/A
         Port
         Hello Time N/A    Max Age N/A       Forward Delay N/A


Bridg    Prior             36864
e ID     ity
         Addre             00:02:4b:29:7a:00
         ss
         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Interfaces
Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast
----     -----    -----    -----    ---      ----     -----    ----
         --       ---                                 ---
```

```
g1       Enabl    128.1    20000    -        -        -        -
         ed

g2       Enabl    128.2    20000    -        -        -        -
         ed

g3       Disab    128.3    20000    -        -        -        -
         led

g4       Enabl    128.4    20000    -        -        -        -
         ed

g5       Enabl    128.5    20000    -        -        -        -
         ed


Console# show spanning-tree active


Spanning tree enabled mode RSTP

Default port cost method: long


Root     Prior             32768
ID       ity

         Addre             00:01:42:97:e0:00
         ss

         Path              20000
         Cost

         Root              1 (1)
         Port

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Bridg    Prior             36864
e ID     ity

         Addre             00:02:4b:29:7a:00
         ss

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Interfaces
```

```
Name    State    Prio.   Cost     Sts     Role     PortF   Type
                 Nbr                               ast

----    -----    -----   -----    ---     ----     -----   -----
        --       ---                               ---     -----

g1      Enabl    128.1   20000    FWD     Root     No      P2p
        ed                                                 (RSTP
                                                           )

g2      Enabl    128.2   20000    FWD     Desg     No      Share
        ed                                                 d
                                                           (STP)

g4      Enabl    128.4   20000    BLK     ALTN     No      Share
        ed                                                 d
                                                           (STP)


Console# show spanning-tree blockedports


Spanning tree enabled mode RSTP

Default port cost method: long


Root    Prior            32768
ID      ity

        Addre            00:01:42:97:e0:00
        ss

        Path             20000
        Cost

        Root             1 (1)
        Port

        Hello Time 2     Max Age 20 sec   Forward Delay 15 sec
        sec


Bridg   Prior            36864
e ID    ity

        Addre            00:02:4b:29:7a:00
        ss

        Hello Time 2     Max Age 20 sec   Forward Delay 15 sec
        sec
```

```
Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----

g4       Enabl    128.4    20000    BLK      ALTN     No       Share
         ed                                                    d
                                                               (STP)


Console# show spanning-tree detail


Spanning tree enabled mode RSTP

Default port cost method: long


Root     Prior             32768
ID       ity

         Addre             00:01:42:97:e0:00
         ss

         Path              20000
         Cost

         Root              1 (1)
         Port

         Hello Time 2      Max Age 20 sec   Forward Delay 15 sec
         sec


Bridg    Prior    36864
e ID     ity

         Addre             00:02:4b:29:7a:00
         ss

         Hello Time 2      Max Age 20 sec   Forward Delay 15 sec
         sec


Number of topology changes 2 last change occurred 2d18h ago
```

```
Times    hold 1, topology change 35, notification 2
:
         hello 2, max age 20, forward delay 15


Port 1 (1) enabled
State: Forwarding                  Role: Root
Port id: 128.1                     Port cost: 20000
Type: P2p (configured: auto)       Port Fast: No (configured:no)
RSTP
Designated bridge Priority:        Address: 00:01:42:97:e0:00
32768
Designated port id: 128.25         Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 2 (2) enabled
State: Forwarding                  Role: Designated
Port id: 128.2                     Port cost: 20000
Type: Shared (configured: auto)    Port Fast: No (configured:no)
STP
Designated bridge Priority:        Address: 00:02:4b:29:7a:00
32768
Designated port id: 128.2          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 3 (3) disabled
State: N/A                         Role: N/A
Port id: 128.3                     Port cost: 20000
Type: N/A (configured: auto)       Port Fast: N/A (configured:no)
Designated bridge Priority: N/A    Address: N/A
Designated port id: N/A            Designated path cost: N/A
```

```
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A


Port 4 (4) enabled
State: Blocking                   Role: Alternate
Port id: 128.4                    Port cost: 20000
Type: Shared (configured:auto)    Port Fast: No (configured:no)
STP
Designated bridge Priority:       Address: 00:30:94:41:62:c8
28672
Designated port id: 128.25        Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 5 (5) enabled
State: Disabled                   Role: N/A
Port id: 128.5                    Port cost: 20000
Type: N/A (configured: auto)      Port Fast: N/A (configured:no)
Designated bridge Priority: N/A   Address: N/A
Designated port id: N/A           Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
```

```
Console# show spanning-tree ethernet 1

Port 1 (1) enabled

State: Forwarding                 Role: Root

Port id: 128.1                    Port cost: 20000

Type: P2p (configured: auto)      Port Fast: No (configured:no)
RSTP

Designated bridge Priority:       Address: 00:01:42:97:e0:00
32768

Designated port id: 128.25        Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Console# show spanning-tree mst-configuration


Name: Region1

Revision: 1

Instance         Vlans mapped     State

--------         ------------     -----
                                  --

g0               1-9, 21-4094     Enabl
                                  ed

g1               10-20            Enabl
                                  ed


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior   32768
                 ity
```

```
                    Address     00:01:42:97:e0:00
                    Path Cost   20000
                    Root Port   1 (1)
                    Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec


Interfaces
Name    State     Prio.Nbr  Cost    Sts   Role   PortFast   Type
----    -------   --------  -----   ---   ----   --------   ----------
g1      Enabled   128.1     20000   FWD   Root   No         P2p Bound(RSTP)
g2      Enabled   128.2     20000   FWD   Desg   No         Shared Bound(STP)
g3      Enabled   128.3     20000   FWD   Desg   No         P2p
g4      Enabled   128.4     20000   FWD   Desg   No         P2p


###### MST 1 Vlans Mapped: 10-20
CST Root ID         Priority    24576
                    Address     00:02:4b:29:89:76
                    Path Cost   20000
                    Root Port   g4 (4)
```

```
                  Rem      19
                  hops


Bridge ID         Prior    32768
                  ity

                  Addre    00:02:4b:29:7a
                  ss       :00


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----

g1       Enabl    128.1    20000    FWD      Boun     No       P2p
         ed                                                    Bound
                                                               (RSTP
                                                               )

g2       Enabl    128.2    20000    FWD      Boun     No       Share
         ed                                                    d
                                                               Bound
                                                               (STP)

g3       Enabl    128.3    20000    BLK      Altn     No       P2p
         ed

g4       Enabl    128.4    20000    FWD      Desg     No       P2p
         ed


Console# show spanning-tree detail


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID       Prior    32768
                  ity

                  Addre    00:01:42:97:e0:00
                  ss
                  Path    20000
                  Cost

                  Root    1 (g1)
                  Port

                  Hello Time 2     Max Age 20 sec   Forward Delay
                  sec                               15 sec



Port 1 (g1) enabled

State: Forwarding                          Role: Root

Port id: 128.1                             Port cost: 20000

Type: P2p (configured: auto) Boundary      Port Fast: No
RSTP                                       (configured:no)

Designated bridge Priority:                Address:
32768                                      00:01:42:97:e0:00

Designated port id: 128.25                 Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (g2) enabled

State: Forwarding                          Role: Designated

Port id: 128.2                             Port cost: 20000

Type: Shared (configured: auto) Boundary   Port Fast: No
STP                                        (configured:no)

Designated bridge Priority:                Address:
32768                                      00:02:4b:29:7a:00

Designated port id: 128.2                  Designated path cost:
                                           20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638
```

```
Port 3 (g3) enabled

State: Forwarding                           Role: Designated

Port id: 128.3                              Port cost: 20000

Type: Shared (configured: auto) Internal    Port Fast: No
                                            (configured:no)

Designated bridge Priority:                 Address:
32768                                       00:02:4b:29:7a:00

Designated port id: 128.3                   Designated path cost:
                                            20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 4 (g4) enabled

State: Forwarding                           Role: Designated

Port id: 128.4                              Port cost: 20000

Type: Shared (configured: auto) Internal    Port Fast: No
                                            (configured:no)

Designated bridge Priority:                 Address:
32768                                       00:02:4b:29:7a:00

Designated port id: 128.2                   Designated path cost:
                                            20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20

Root ID          Prior    24576
                 ity

                 Addre    00:02:4b:29:89:76
                 ss

                 Path     20000
                 Cost

                 Port     4 (4)
                 Cost

                 Rem      19
                 hops
```

```
Bridge ID       Prior    32768
                ity

                Addre    00:02:4b:29:7a:00
                ss

                Number of topology changes 2 last change
                occurred 1d9h ago

                Times:  hold 1, topology change 2, notification 2
                hello 2, max age 20, forward delay 15


Port 1 (g1) enabled

State: Forwarding                         Role: Boundary

Port id: 128.1                            Port cost: 20000

Type: P2p (configured: auto) Boundary     Port Fast: No
RSTP                                      (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.1                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (g2) enabled

State: Forwarding                         Role: Designated

Port id: 128.2                            Port cost: 20000

Type: Shared (configured: auto) Boundary  Port Fast: No
STP                                       (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.2                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638
```

```
Port 3 (g3) disabled

State: Blocking                           Role: Alternate

Port id: 128.3                            Port cost: 20000

Type: Shared (configured: auto) Internal  Port Fast: No
                                          (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:1a:19

Designated port id: 128.78                Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 4 (g4) enabled

State: Forwarding                         Role: Designated

Port id: 128.4                            Port cost: 20000

Type: Shared (configured: auto) Internal  Port Fast: No
                                          (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.2                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior    32768
                 ity

                 Addre    00:01:42:97:e0:00
                 ss
                 Path     20000
                 Cost

                 Root     1 (g1)
                 Port

                 Hello Time 2     Max Age 20 sec   Forward Delay
                 sec                               15 sec


Bridg            Prior    32768
e ID             ity

                 Addre    00:02:4b:29:7a
                 ss       :00

                 Hello Time 2     Max Age 20 sec   Forward Delay
                 sec                               15 sec

                 Max      20
                 hops


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior    32768
                 ity

                 Addre    00:01:42:97:e0:00
                 ss
```

```
Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: short


CST      Prior            32768
Root     ity
ID

         Addre            00:01:42:97:e0:00
         ss

         Path             20000
         Cost

         Root             1 (1)
         Port

Bridg    Prior            36864
e ID     ity

         Addre            00:02:4b:29:7a:00
         ss

         Hello Time 2     Max Age 20 sec   Forward Delay 15 sec
         sec

         Max              20
         hops

Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----

g1       Enabl    128.1    20000    FWD      Root     No       P2p
         ed                                                    bound
                                                               (RSTP
                                                               )

g2       Enabl    128.2    20000    FWD      Desg     No       Share
         ed                                                    d
                                                               (STP)

g3       Disab    128.3    20000    -        -        -        -
         led
```

```
g4       Enabl    128.4    20000    BLK      ALTN     No       Share
         ed                                                    d
                                                               (STP)

g5       Enabl    128.5    20000    DIS      -        -        -
         ed


Console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: long


Root     Prior             36864
ID       ity

         Addre             00:02:4b:29:7a:00
         ss

         This switch is the root.

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----

g1       Enabl    128.1    20000    FWD      Desg     No       P2p
         ed                                                    (RSTP
                                                               )

g2       Enabl    128.2    20000    FWD      Desg     No       Share
         ed                                                    d
                                                               (STP)

g3       Disab    128.3    20000    -        -        -        -
         led

g4       Enabl    128.4    20000    FWD      Desg     No       Share
         ed                                                    d
                                                               (STP)
```

```
g5       Enabl    128.5    20000    DIS      -        -        -
         ed


Console# show spanning-tree


Spanning tree disabled (BPDU filtering) mode RSTP

Default port cost method: long


Root     Prior             N/A
ID       ity

         Addre             N/A
         ss

         Path              N/A
         Cost

         Root              N/A
         Port

         Hello Time N/A    Max Age N/A       Forward Delay N/A


Bridg    Prior             36864
e ID     ity

         Addre             00:02:4b:29:7a:00
         ss

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    ----
         --       ---                                 ---

g1       Enabl    128.1    20000    -        -        -        -
         ed

g2       Enabl    128.2    20000    -        -        -        -
         ed
```

```
g3       Disab    128.3    20000    -        -        -        -
         led

g4       Enabl    128.4    20000    -        -        -        -
         ed

g5       Enabl    128.5    20000    -        -        -        -
         ed


Console# show spanning-tree active


Spanning tree enabled mode RSTP

Default port cost method: long


Root     Prior             32768
ID       ity

         Addre             00:01:42:97:e0:00
         ss

         Path              20000
         Cost

         Root              1 (g1)
         Port

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Bridg    Prior             36864
e ID     ity

         Addre             00:02:4b:29:7a:00
         ss

         Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
         sec


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----
```

```
g1      Enabl   128.1   20000   FWD     Root    No      P2p
        ed                                              (RSTP
                                                        )
g2      Enabl   128.2   20000   FWD     Desg    No      Share
        ed                                              d
                                                        (STP)
g4      Enabl   128.4   20000   BLK     ALTN    No      Share
        ed                                              d
                                                        (STP)


Console# show spanning-tree blockedports


Spanning tree enabled mode RSTP
Default port cost method: long


Root    Prior           32768
ID      ity
        Addre           00:01:42:97:e0:00
        ss
        Path            20000
        Cost
        Root            1 (1)
        Port
        Hello Time 2    Max Age 20 sec  Forward Delay 15 sec
        sec


Bridg   Prior           36864
e ID    ity
        Addre           00:02:4b:29:7a:00
        ss
        Hello Time 2    Max Age 20 sec  Forward Delay 15 sec
        sec


Interfaces
Name    State   Prio.   Cost    Sts     Role    PortF   Type
                Nbr                             ast
```

```
----    -----    -----    -----    ---      ----     -----    -----
        --       ---                                 ---      -----

4       Enabl    128.4    20000    BLK      ALTN     No       Share
        ed                                                    d
                                                              (STP)


Console# show spanning-tree detail


Spanning tree enabled mode RSTP

Default port cost method: long


Root    Prior             32768
ID      ity

        Addre             00:01:42:97:e0:00
        ss

        Path              20000
        Cost

        Root              1 (g1)
        Port

        Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
        sec


Bridg   Prior    36864
e ID    ity

        Addre             00:02:4b:29:7a:00
        ss

        Hello Time 2      Max Age 20 sec    Forward Delay 15 sec
        sec


Number of topology changes 2 last change occurred 2d18h ago

Times   hold 1, topology change 35, notification 2
:

        hello 2, max age 20, forward delay 15


Port 1 (g1) enabled
```

```
State: Forwarding                 Role: Root

Port id: 128.1                    Port cost: 20000

Type: P2p (configured: auto)      Port Fast: No (configured:no)
RSTP

Designated bridge Priority:       Address: 00:01:42:97:e0:00
32768

Designated port id: 128.25        Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (g2) enabled

State: Forwarding                 Role: Designated

Port id: 128.2                    Port cost: 20000

Type: Shared (configured: auto)   Port Fast: No (configured:no)
STP

Designated bridge Priority:       Address: 00:02:4b:29:7a:00
32768

Designated port id: 128.2         Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 3 (g3) disabled

State: N/A                        Role: N/A

Port id: 128.3                    Port cost: 20000

Type: N/A (configured: auto)      Port Fast: N/A (configured:no)

Designated bridge Priority: N/A   Address: N/A

Designated port id: N/A           Designated path cost: N/A

Number of transitions to forwarding state: N/A

BPDU: sent N/A, received N/A


Port 4 (g4) enabled

State: Blocking                   Role: Alternate
```

```
Port id: 128.4                    Port cost: 20000

Type: Shared (configured:auto)    Port Fast: No (configured:no)
STP

Designated bridge Priority:       Address: 00:30:94:41:62:c8
28672

Designated port id: 128.25        Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 5 (g5) enabled

State: Disabled                   Role: N/A

Port id: 128.5                    Port cost: 20000

Type: N/A (configured: auto)      Port Fast: N/A (configured:no)

Designated bridge Priority: N/A   Address: N/A

Designated port id: N/A           Designated path cost: N/A

Number of transitions to forwarding state: N/A

BPDU: sent N/A, received N/A


Console# show spanning-tree ethernet 1

Port 1 (g1) enabled

State: Forwarding                 Role: Root

Port id: 128.1                    Port cost: 20000

Type: P2p (configured: auto)      Port Fast: No (configured:no)
RSTP

Designated bridge Priority:       Address: 00:01:42:97:e0:00
32768

Designated port id: 128.25        Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

```
Console# show spanning-tree mst-configuration


Name: Region1

Revision: 1

Instance         Vlans mapped     State

--------         ------------     -----
                                  --

g0               1-9, 21-4094     Enabl
                                  ed

g1               10-20            Enabl
                                  ed


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior    32768
                 ity

                 Addre    00:01:42:97:e0:00
                 ss

                 Path     20000
                 Cost

                 Root     1 (g1)
                 Port

                 Hello Time 2     Max Age 20 sec    Forward Delay
                 sec                                15 sec


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----
```

```
g1       Enabl    128.1    20000    FWD      Root     No       P2p
         ed                                                    Bound
                                                               (RSTP
                                                               )

g2       Enabl    128.2    20000    FWD      Desg     No       Share
         ed                                                    d
                                                               Bound
                                                               (STP)

g3       Enabl    128.3    20000    FWD      Desg     No       P2p
         ed

g4       Enabl    128.4    20000    FWD      Desg     No       P2p
         ed


###### MST 1 Vlans Mapped: 10-20

CST Root ID       Prior    24576
                  ity

                  Addre    00:02:4b:29:89:76
                  ss

                  Path     20000
                  Cost

                  Root     4 (g4)
                  Port

                  Rem      19
                  hops


Bridge ID         Prior    32768
                  ity

                  Addre    00:02:4b:29:7a
                  ss       :00


Interfaces

Name     State    Prio.    Cost     Sts      Role     PortF    Type
                  Nbr                                 ast

----     -----    -----    -----    ---      ----     -----    -----
         --       ---                                 ---      -----
```

```
g1       Enabl    128.1    20000    FWD      Boun     No       P2p
         ed                                                    Bound
                                                               (RSTP
                                                               )

g2       Enabl    128.2    20000    FWD      Boun     No       Share
         ed                                                    d
                                                               Bound
                                                               (STP)

g3       Enabl    128.3    20000    BLK      Altn     No       P2p
         ed

g4       Enabl    128.4    20000    FWD      Desg     No       P2p
         ed


Console# show spanning-tree detail


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID       Prior    32768
                  ity

                  Addre    00:01:42:97:e0:00
                  ss

                  Path     20000
                  Cost

                  Root     1 (g1)
                  Port

                  Hello Time 2      Max Age 20 sec   Forward Delay
                  sec                                15 sec



Port 1 (g1) enabled

State: Forwarding                           Role: Root

Port id: 128.1                              Port cost: 20000

Type: P2p (configured: auto) Boundary       Port Fast: No
RSTP                                        (configured:no)
```

```
Designated bridge Priority:               Address:
32768                                     00:01:42:97:e0:00

Designated port id: 128.25                Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (g2) enabled

State: Forwarding                         Role: Designated

Port id: 128.2                            Port cost: 20000

Type: Shared (configured: auto) Boundary  Port Fast: No
STP                                       (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.2                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 3 (g3) enabled

State: Forwarding                         Role: Designated

Port id: 128.3                            Port cost: 20000

Type: Shared (configured: auto) Internal  Port Fast: No
                                          (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.3                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 4 (g4) enabled

State: Forwarding                         Role: Designated

Port id: 128.4                            Port cost: 20000
```

```
Type: Shared (configured: auto) Internal   Port Fast: No
                                           (configured:no)

Designated bridge Priority:                Address:
32768                                      00:02:4b:29:7a:00

Designated port id: 128.2                  Designated path cost:
                                           20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20

Root ID          Prior    24576
                 ity

                 Addre    00:02:4b:29:89:76
                 ss

                 Path     20000
                 Cost

                 Port     4 (4)
                 Cost

                 Rem      19
                 hops


Bridge ID        Prior    32768
                 ity

                 Addre    00:02:4b:29:7a:00
                 ss

                 Number of topology changes 2 last change
                 occurred 1d9h ago

                 Times:  hold 1, topology change 2, notification 2
                 hello 2, max age 20, forward delay 15


Port 1 (g1) enabled

State: Forwarding                          Role: Boundary

Port id: 128.1                             Port cost: 20000

Type: P2p (configured: auto) Boundary      Port Fast: No
RSTP                                       (configured:no)
```

```
Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.1                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (g2) enabled

State: Forwarding                         Role: Designated

Port id: 128.2                            Port cost: 20000

Type: Shared (configured: auto) Boundary  Port Fast: No
STP                                       (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.2                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 3 (g3) disabled

State: Blocking                           Role: Alternate

Port id: 128.3                            Port cost: 20000

Type: Shared (configured: auto) Internal  Port Fast: No
                                          (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:1a:19

Designated port id: 128.78                Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 4 (g4) enabled

State: Forwarding                         Role: Designated

Port id: 128.4                            Port cost: 20000
```

```
Type: Shared (configured: auto) Internal  Port Fast: No
                                          (configured:no)

Designated bridge Priority:               Address:
32768                                     00:02:4b:29:7a:00

Designated port id: 128.2                 Designated path cost:
                                          20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior    32768
                 ity

                 Addre    00:01:42:97:e0:00
                 ss

                 Path     20000
                 Cost

                 Root     1 (g1)
                 Port

                 Hello Time 2     Max Age 20 sec   Forward Delay
                 sec                               15 sec


Bridg            Prior    32768
e ID             ity

                 Addre    00:02:4b:29:7a
                 ss       :00

                 Hello Time 2     Max Age 20 sec   Forward Delay
                 sec                               15 sec

                 Max      20
                 hops
```

```
Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID      Prior   32768
                 ity

                 Addre   00:01:42:97:e0:00
                 ss
```

16 CONFIGURATION AND IMAGE FILE COMMANDS

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

Syntax

copy source-url destination-url

Parameters

- *source-url* — The source file location URL or reserved keyword of the source file to be copied. (Range: 1-160 characters)
- *destination-url* — The destination file URL or reserved keyword of the destination file. (Range: 1-160 characters)

The following table displays keywords and URL prefixes.

Keyword	Source or Destination
flash:	Source or destination URL for flash memory. It's the default in case a URL is specified without a prefix.
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
image	If the source file, represents the active image file. If the destination file, represents the non-active image file.
boot	Boot file.
tftp://	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**//*host*/*[directory]*/*filename*. The host can be represented by its IP address or hostname.

Keyword	Source or Destination
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

*.prv and *.sys files cannot be copied.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy if one of the following conditions exist:

The source file and destination file are the same file.

xmodem: is the destination file. The source file can be copied to **image**, **boot** and **null**: only.

tftp:// is the source file and destination file on the same copy.

The following table describes copy characters:

Character	Description
!	For network transfers, indicates that the copy process is taking place. Eac point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out. General in a row means that the copy process may fail.

Copying an Image File from a Server to Flash Memory

To copy an image file from a server to flash memory, use the **copy** source-url **image** command.

Copying a Boot File from a Server to Flash Memory

To copy a boot file from a server to flash memory, enter the **copy** *source-url* **boot** command.

Copying a Configuration File from a Server to the Running Configuration File

To load a configuration file from a network server to the running configuration file of the device, enter the **copy** *source-url* **running-config** command. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file is a combination of the previous running configuration and the loaded configuration files with the loaded configuration file taking precedence.

Copying a Configuration File from a Server to the Startup Configuration To copy a configuration file from a network server to the startup configuration file of the device, enter **copy** *source-url* **startup-config**. The startup configuration file is replaced by the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy running-config** *destination-url* command to copy the current configuration file to a network server using TFTP. Use the **copy startup-config** *destination-url* command to copy the startup configuration file to a network server.

Saving the Running Configuration to the Startup Configuration

To copy the running configuration to the startup configuration file, enter the **copy running-config startup-config** command.

Example

The following example copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```
Console# copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

Syntax

delete *url*

Parameters

- *url* — The location URL or reserved keyword of the file to be deleted. (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash:	Source or destination URL for flash memory. It’s the default in case a URL is specified without a prefix.
startup-config	Represents the startup configuration file.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

*.sys, *.prv, image-1 and image-2 files cannot be deleted.

Example

The following example deletes the file called ‘test’ from the flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```

boot system

The **boot system** Privileged EXEC mode command specifies the system image that the device loads at startup.

Syntax

boot system {**image-1** | **image-2**}

Parameters

- **image-1** — Specifies image 1 as the system startup image.
- **image-2** — Specifies image 2 as the system startup image.

Default Configuration

The default setting is the unit number.

Command Mode

Privileged EXEC mode

User Guidelines

Use the show bootvar command to find out which image is the active image.

Example

The following example loads the system image 1 at device startup.

```
Console# boot system image-1
```

show running-config

The **show running-config** Privileged EXEC mode command displays the contents of the currently running configuration file.

Syntax

show running-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the contents of the running configuration file.

```
Console# show running-config

hostname device

interface ethernet g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000

interface ethernet g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

show startup-config

The **show startup-config** Privileged EXEC mode command displays the contents of the startup configuration file.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the contents of the running configuration file.

```
Console# show startup-config

hostname device

interface ethernet g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000

interface ethernet g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

show bootvar

The **show bootvar** Privileged EXEC mode command displays the active system image file that is loaded by the device at startup.

Syntax

show bootvar Elana

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the active system image file that is loaded by the device at startup. Elana

```
Console# show bootvar


Unit                   Active Image           Selected for next
                                              boot

----                   ------------           --------------------
                                              --

1                      image-1                image-1

2                      image-2                image-2

3                      image-1                image-1
```

17 RADIUS COMMAND

radius-server host

The **radius-server host** Global Configuration mode command specifies a RADIUS server host. To delete the specified RADIUS host, use the **no** form of this command.

Syntax

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*] [**usage** *type*]

no radius-server host {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the RADIUS server host.
- *hostname* — Hostname of the RADIUS server host. (Range: 1-158 characters)
- *auth-port-number* — Port number for authentication requests. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)
- *retries* — Specifies the retransmit value. (Range: 1-10)
- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)
- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter " ". (Range: 0-128 characters)

- *source* — Specifies the source IP address to use for communication. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
- *priority* — Determines the order in which servers are used, where 0 has the highest priority. (Range: 0-65535)
- *type* — Specifies the usage type of the server. Possible values: **login**, **dot.1x**, **wireless** or **all**.

Default Configuration

No RADIUS server host is specified.

The port number for authentication requests is 1812.

The usage type is **all**.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific timeout, retries, deadtime or key-string values are specified, global values apply to each RADIUS server host.

The address type of the source parameter must be the same as the **ip-address** parameter.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20 and a 20-second timeout period.

```
Console(config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

radius-server key

The **radius-server key** Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To restore the default configuration, use the **no** form of this command.

Syntax

radius-server key [*key-string*]

no radius-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0-128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key enterprise-server
```

radius-server retransmit

The **radius-server retransmit** Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

Parameters

- *retries* — Specifies the retransmit value. (Range: 1-10)

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the number of times the software searches all RADIUS server hosts to 5 times.

```
console(config)# radius-server retransmit 5
```

radius-server source-ip

The **radius-server source-ip** Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. To restore the default configuration, use the **no** form of this command.

Syntax

radius-server source-ip *source*

no radius-source-ip *source*

Parameters

- *source* — Specifies a valid source IP address.

Default Configuration

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
console(config)# radius-server source-ip 10.1.1.1
```

radius-server timeout

The **radius-server timeout** Global Configuration mode command sets the interval during which the device waits for a server host to reply. To restore the default configuration, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)

Default Configuration

The timeout value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the timeout interval on all RADIUS servers to 5 seconds.

```
Console(config)# radius-server timeout 5
```

radius-server deadtime

The **radius-server deadtime** Global Configuration mode command improves RADIUS response time when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To restore the default configuration, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameters

- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)

Default Configuration

The deadtime setting is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets all RADIUS server deadtimes to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

show radius-servers

The **show radius-servers** Privileged EXEC mode command displays the RADIUS server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RADIUS server settings.

```
Console# show radius-servers


IP       Port     TimeO    Retra    DeadT    Sourc    Prior    Usage
addre    Auth     ut       nsmit    ime      e IP     ity
ss

-----    ----     -----    -----    -----    -----    -----    -----
----              --       -----    -        ---      ---

172.1    1645     Globa    Globa    Globa    -        1        All
6.1.1             l        l        l

172.1    1645     11       8        Globa    Globa    2        All
6.1.2                               l        l


Global values

-------------

TimeOut: 3

Retransmit: 3

Deadtime: 0

Source IP: 172.16.8.1
```

18 PORT MONITOR COMMANDS

port monitor

The **port monitor** Interface Configuration mode command starts a port monitoring session. To stop a port monitoring session, use the **no** form of this command.

Syntax

port monitor *src-interface* [**rx | tx**]

no port monitor *src-interface*

Parameters

- *src-interface* — Valid Ethernet port.Elana
- **rx —** *Monitors received packets only.*
- **tx —** *Monitors transmitted packets only.*

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables traffic on one port to be copied to another port, or between the source port (*src-interface) and a destination port (port being configured).*

The following restrictions apply to ports configured as destination ports:

The port cannot be already configured as a source port.

The port cannot be a member in a port-channel.

An *IP interface is not configured on the port.*

GVRP is not enabled on the port.

The port is not a member of a VLAN, except for the default VLAN (will automatically be removed from the default VLAN).

The f*ollowing restrictions apply to ports configured to be source ports:*

The port cannot be already configured as a destination port.

Maximum number of source ports can be up to eight.

Example

The following example copies traffic for both directions (Tx and Rx) on port g8 (source port) to port 1 (destination port).

```
Console(config)# interface ethernet g1
Console(config-if)# port monitor g8
```

show ports monitor

The **show ports monitor** Privileged EXEC mode command displays the port monitoring status.

Syntax

show ports monitor

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how the port monitoring status is displayed.

```
Console# show ports monitor



Source        Destinatio   Type          Status
Port          n Port
```

```
----------    ----------    -----         -------
-             ------

g1            8             RX,TX         Active

g2            8             RX,TX         Active

g18           8             RX            Active
```

19 SNMP COMMANDS

snmp-server community

The **snmp-server community** Global Configuration mode command configures the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*] [**view** *view-name*]

snmp-server community-group *community group-name* [*ip-address*]

no snmp-server community *community* [*ip-address*]

Parameters

- *community* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro** — Indicates read-only access (default).
- **rw** — Indicates read-write access.
- **su** — Indicates SNMP administrator access.
- *ip-address* — Specifies the IP address of the management station.
- *group-name* — Specifies the name of a previously defined group. A group defines the objects available to the community. (Range: 1-30 characters)
- *view-name* — Specifies the name of a previously defined view. The view defines the objects available to the community. (Range: 1-30 characters).

Default Configuration

No communities are defined.

Command Mode

Global Configuration mode

User Guidelines

The **view-name** parameter cannot be specified for su, which has access to the whole MIB.

The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.

The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view-name (read-view and notify-view always, and for **rw** for write-view also)

The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to the group name.

Example

The following example defines community access string **public** to permit administrative access to SNMP protocol at an administrative station with IP address 192.168.1.20.

```
Console(config)# snmp-server community public su 192.168.1.20
```

snmp-server view

The **snmp-server view** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. To remove a specified SNMP server view entry, use the **no** form of this command.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name* [*oid-tree*]

Parameters

- *view-name* — Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included** — Indicates that the view type is included.
- **excluded** — Indicates that the view type is excluded.

Default Configuration

No view entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view record.

The number of views is limited to 64.

No check is made to determine that a MIB node corresponds to the "starting portion" of the OID until the first wildcard.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1
included
```

snmp-server group

The **snmp-server group** Global Configuration mode command configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.

Syntax

snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*]} [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* {**v1** | **v2** | **v3** [**noauth** | **auth** | **priv**]}

Parameters

- *groupname*—Specifies the name of the group (Range: 1-30 characters).
- **v1** — Indicates the SNMP Version 1 security model.
- **v2** — Indicates the SNMP Version 2 security model.
- **v3** — Indicates the SNMP Version 3 security model.
- **noauth** — Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth** — Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv** — Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- *name* — Specifies the context of a packet. The following context is supported: Router. If the context name is unspecified, all contexts are defined.
- *readview* — Specifies a string that is the name of the view that enables only viewing the contents of the agent. If unspecified, all objects except for the community-table and SNMPv3 user and access tables are available.
- *writeview* — Specifies a string that is the name of the view that enables entering data and configuring the contents of the agent. If unspecified, nothing is defined for the write view.
- *notifyview* — Specifies a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. Applicable only to the SNMP Version 3 security model.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

```
Console(config)# snmp-server group user-group v3 priv read
user-view
```

snmp-server user

The **snmp-server user** Global Configuration mode command configures a new SNMP Version 3 user. To remove a user, use the **no** form of this command.

Syntax

snmp-server user *username groupname* [**remote** *engineid-string*] [**auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-des-keys* | **auth-sha-key** *sha-des-keys*]

no snmp-server user *username* [**remote** *engineid-string*]

Parameters

- *username* — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters)
- *groupname* — Specifies the name of the group to which the user belongs. (Range: 1-30 characters)
- *engineid-string* — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 5-32 characters)

- **auth-md5** *password* — Indicates the HMAC-MD5-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-sha** *password*—Indicates the HMAC-SHA-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-md5-key** *md5-des-keys* — Indicates the HMAC-MD5-96 authentication level. The user should enter a concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required, 16 bytes should be entered; if authentication and privacy are required, 32 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (16 or 32 bytes)
- **auth-sha-key** *sha-des-keys* — Indicates the HMAC-SHA-96 authentication level. The user should enter a concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required, 20 bytes should be entered; if authentication and privacy are required, 36 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (20 or 36 bytes)

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

If auth-md5 or auth-sha is specified, both authentication and privacy are enabled for the user.

When a **show running-config** Privileged EXEC mode command is entered, a line for this user will not be displayed. To see if this user has been added to the configuration, type the **show snmp users** Privileged EXEC mode command.

An SNMP EngineID has to be defined to add SNMP users to the device. Changing or removing the SNMP EngineID value deletes SNMPv3 users from the device’s database.

The remote engineid designates the remote management station and should be defined to enable the device to receive informs.

Example

The following example configures an SNMPv3 user John in a group called user-group.

```
Console(config)# snmp-server user John user-group
```

snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. To remove the configured engine ID, use the **no** form of this command.

Syntax

snmp-server engineID local {*engineid-string* | **default**}

no snmp-server engineID local

Parameters

- *engineid-string*—Specifies a character string that identifies the engine ID. (Range: 5-32 characters)
- **default**—The engine ID is created automatically based on the device MAC address.

Default Configuration

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- First 4 octets — first bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet — set to 3 to indicate the MAC address that follows.
- Last 6 octets — MAC address of the device.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.

If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify snmp-server engineID local 1234.

Since the engine ID should be unique within an administrative domain, the following is recommended:

For a standalone device, use the default keyword to configure the engine ID.

Changing the value of the engine ID has the following important side-effect. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user’s command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x000000001.

The **show running-config** Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the **snmp-server engineID l**ocal Global Configuration mode command.

Example

The following example enables SNMPv3 on the device and sets the local engine ID of the device to the default value.

```
Console(config) # snmp-server engineID local default
```

snmp-server enable traps

The **snmp-server enable traps** Global Configuration mode command enables the device to send SNMP traps. To disable SNMP traps, use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP traps.

```
Console(config)# snmp-server enable traps
```

snmp-server filter

The **snmp-server filter** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree* {**included** | **excluded**}

no snmp-server filter *filter-name* [*oid-tree*]

Parameters ■

- *filter-name* — Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a

text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.

- **included** — Indicates that the filter type is included.
- **excluded** — Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system
included
Console(config)# snmp-server filter filter-name system.7
excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1
included
```

snmp-server host

The **snmp-server host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server host {*ip-address* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds]* [**retries** *retries*]

no snmp-server host {ip-*address* | *hostname*} [**traps** | **informs**]

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *community-string* — Specifies a password-like community string sent with the notification operation.
- (Range: 1-20)
- **traps** — Indicates that SNMP traps are sent to this host. If unspecified, SNMPv2 traps are sent to the host.
- **informs** — Indicates that SNMP informs are sent to this host. Not applicable to SNMPv1.
- **1** — Indicates that SNMPv1 traps will be used.
- **2** — Indicates that SNMPv2 traps will be used. If
- port—Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162.
- (Range:1-65535)
- *filtername* — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered.

  (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds.

  (Range: 1-300)
- *retries* — Specifies the maximum number of times to resend an **inform** request. If unspecified, the default maximum number of retries is 3. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

When configuring an SNMPv1 or SNMPv2 notification recipient, a notification view for that recipient is automatically generated for all the MIB.

When configuring an SNMPv1 notification recipient, the Inform option cannot be selected.

If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.

Example

The following example enables SNMP traps for host 10.1.1.1 with community string "management" using SNMPv2.

```
Console(config)# snmp-server host 10.1.1.1 management 2
```

snmp-server v3-host

The **snmp-server v3-host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server v3-host {*ip-address* | *hostname*} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]

no snmp-server host {*ip-address* | *hostname*} *username* [**traps** | **informs**]

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *username* — Specifies the name of the user to use to generate the notification. (Range: 1-24)
- **traps** — Indicates that SNMP traps are sent to this host.
- **informs** — Indicates that SNMP informs are sent to this host.
- **noauth** — Indicates no authentication of a packet.
- **auth** — Indicates authentication of a packet without encrypting it.

- **priv** — Indicates authentication of a packet with encryption.
- *port* — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- *filtername*—Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- *retries* — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

A user and notification view are not automatically created. Use the **snmp-server user**, **snmp-server group** and **snmp-server view** Global Configuration mode commands to generate a user, group and notify group, respectively.

Example

The following example configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```

snmp-server trap authentication

The **snmp-server trap authentication** Global Configuration mode command enables the device to send SNMP traps when authentication fails. To disable SNMP failed authentication traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

snmp-server contact

The **snmp-server contact** Global Configuration mode command configures the system contact (sysContact) string. To remove system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

- *text* — Specifies the string that describes system contact information. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example configures the system contact point called **3Com_Technical_Support**.

```
console(config)# snmp-server contact 3Com_Technical_Support
```

snmp-server location

The **snmp-server location** Global Configuration mode command configures the system location string. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

Parameters

- *text* — Specifies a string that describes system location information. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example defines the device location as **New_York**.

```
Console(config)# snmp-server location New_York
```

snmp-server set

The **snmp-server set** Global Configuration mode command defines the SNMP MIB value.

Syntax

snmp-server set *variable-name name1 value1* [*name2 value2 …*]

Parameters

- *variable-name* — MIB variable name (Range 1-160 characters).
- *name value* — List of name and value pairs. In the case of scalar MIBs, only a single pair of name values. In the case of an entry in a table, at least one pair of name and value followed by one or more fields (Range 1-160 characters).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the **snmp-server se**t command is used.

This command is case-sensitive.

Example

The following example configures the scalar MIB sysName with the value **3Com.**

```
Console(config)# snmp-server set sysName sysname 3Com
```

show snmp

The **show snmp** Privileged EXEC mode command displays the SNMP status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP communications status.

```
Console# show snmp


Commu   Community-Ac   View    IP
nity-   cess           name    addre
Stri                           ss
ng

-----   ----------     -----   -----
-----                  ----    ---

publi   read only      user-   All
c                      view

priva   read write     Defau   172.16.1.1
te                     lt

priva   su             Defau   172.17.1.1
te                     ltSup
                       er


Community-st           Group   IP address     Type
ring                   name

------------           -----   ----------
----                   -----

publi                  user-   all
c                      group


Traps are enabled.

Authentication trap is enabled.
```

```
Version 1,2 notifications

Target         Type    Commu   Versi   UDP     Filte   TO      Retr
Address                nity    on      Port    r       Sec     ies
                                               Name

-----------    -----   -----   -----   ----    -----   ---     ----
--                     ----    --              -               ---

192.122.173.   Trap    publi   2       162             15      3
42                     c

192.122.173.   Infor   publi   2       162             15      3
42             m       c


Version 3 notifications

Target         Type    Usern   Secu    UDP     Filte   TO      Retr
Address                ame     rity    Port    r       Sec     ies
                               Level           Name

-----------    -----   -----   -----   ----    -----   ---     ----
--                     ----    --              -               ---

192.122.173.   Infor   Bob     Priv    162             15      3
42             m


System Contact: Robert

System Location: Marketing
```

The following table describes the significant fields shown in the display.

Field	Description
Community-string	Community access string to permit access to the SNMP protoco
Community-access	Type of access - read-only, read-write, super access
IP Address	Management station IP Address.
Trap-Rec-Address	Targeted Recipient
Trap-Rec-Community	Statistics sent with the notification operation.
Version	SNMP version for the sent trap 1 or 2.

show snmp engineid

The **show snmp engineID** Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP engine ID.

```
Console# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
```

show snmp views

The **show snmp views** Privileged EXEC mode command displays the configuration of views.

Syntax

show snmp views [*viewname*]

Parameters ■

- *viewname* — Specifies the name of the view. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp views


Name                 OID Tree             Type

-----------          -------------------- ---------
                     ---

user-view            1.3.6.1.2.1.1        Included

user-view            1.3.6.1.2.1.1.7      Excluded

user-view            1.3.6.1.2.1.2.2.1.*. Included
                     1
```

show snmp groups

The **show snmp groups** Privileged EXEC mode command displays the configuration of groups.

Syntax

s**how snmp groups** [*groupname*]

Parameters

- *groupname*—Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp groups

Name     Security                    Views
```

```
         Model    Level              Read     Write    Notify
-------  -----    -----              -------  -------  -------
-------
user-gr  V3       priv               Default  ""       ""
oup
manager  V3       priv               Default  Default  ""
s-group
manager  V3       priv               Default  ""       ""
s-group
```

The following table describes significant fields shown above.

Field		**Description**
Name		Name of the group.
Security Model		SNMP model in use (v1, v2 or v3).
Security Level		Authentication of a packet with encryption. Applicable only to SNMP v3 security.
Views	Read	Name of the view that enables only viewing the contents of the agent. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	Name of the view that enables entering data and managing the contents of the agent.
	Notify	Name of the view that enables specifying an inform or a trap.

show snmp filters

The **show snmp filters** Privileged EXEC mode command displays the configuration of filters.

Syntax

show snmp filters [*filtername*]

Parameters

- *filtername*—Specifies the name of the filter. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of filters.

```
Console# show snmp filters


Name                OID Tree             Type
-----------         -------------------- ---------
                    ---
user-filter         1.3.6.1.2.1.1        Included
user-filter         1.3.6.1.2.1.1.7      Excluded
user-filter         1.3.6.1.2.1.2.2.1.*. Included
                    1
```

show snmp users

The **show snmp users** Privileged EXEC mode command displays the configuration of users.

Syntax

show snmp users [*username*]

Parameters

- *username*—Specifies the name of the user. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of users.

```
Console# show snmp users


Name            Group name        Auth Method       Remote
------          ------------      ---------         --------------
                                                    -----------
John            user-group        md5
John            user-group        md5               08009009020C0B
                                                    099C075879
```

20 IP ADDRESS COMMANDS

ip address

The **ip address** Interface Configuration (default VLAN) mode command sets an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* | *prefix-length*}

no ip address *ip-address*

Parameters

- *ip-address* — Specifies the valid IP address.
- *mask* — Specifies the valid network mask of the IP address.
- *prefix-length* — Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8-30)

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration (default VLAN) mode

User Guidelines

Only the default VLAN get be assigned an IP address.

An IP address cannot be configured for a range of interfaces (range context).

This command is only functional if the device is in Switch mode.

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

ip address dhcp

The **ip address dhcp** Interface Configuration (default VLAN) mode command acquires an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure an acquired IP address, use the *no* form of this command.

Syntax

ip address dhcp [**hostname** *host-name*]

no ip address dhcp

Parameters

- *host-name* — Specifies the name of the host to be placed in the DHCP option 12 field. This name does not have to be the same as the **host name** specified in the hostname Global Configuration mode command. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (default VLAN) mode

User Guidelines

This command is only functional if the device is in Switch mode.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The **ip address dhcp hostname** host-name command is most typically used when the host name is provided by the system administrator.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the globally configured host name of the device. However, **the ip address dhcp hostname** host-name command can be used to place a different host name in the DHCP option 12 field.

The n**o ip address dhcp** command deconfigures any IP address that was acquired, and sends a DHCPRELEASE message.

Example

The following example acquires an IP address for Ethernet port g16 from DHCP.

```
Console(config)# interface ethernet g16
Console(config-if)# ip address dhcp
```

ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (device). To restore the default configuration, use the no form of this command.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

Parameters

- *ip-address* — Specifies the valid IP address of the currently defined default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

This command is only operational in Switch mode.

Example

The following example defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```

show ip interface

The **show ip interface** Privileged EXEC mode command displays the usability status of configured IP interfaces.

Syntax

show ip interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number* |]

Parameters

- *interface-number* — Specifies the valid Ethernet port.
- *vlan-id* — Specifies the valid VLAN number.
- *port-channel number* — Specifies the valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example the displays the configured IP interfaces and their types.

```
Console# show ip interface


Proxy ARP is
disabled
```

```
IP address       I/F              Type             Direct
                                                   Broadcast

-------------                     ---------        --------------
                                                   --

10.7.1.192/24    1                Static           disable

10.7.2.192/24    2                Static           disable
```

arp

The **arp** Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.

Syntax

arp *ip_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number.*}

no arp *ip_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number.*}

Parameters

- *ip_addr* — Valid IP address or IP alias to map to the specified MAC address.
- *hw_addr* — Valid MAC address to map to the specified IP address or IP alias.
- *interface-number* — Valid Ethernet port.
- *vlan-id* — Valid VLAN number.
- *port-channel number.* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuratin mode

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not generally have to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet
6
```

arp timeout

The **arp timeout** Global Configuration mode command configures how long an entry remains in the ARP cache. To restore the default configuration, use the **no** form of this command.

Syntax

arp timeout *seconds*

no arp timeout

Parameters

- *seconds* — Time (in seconds) that an entry remains in the ARP cache. (Range: 1-40000000)

Default Configuration

The default timeout is 60000 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended not to set the timeout value to less than 3600.

Example

The following example configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```

clear arp-cache

The **clear arp-cache** Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

The **show arp** Privileged EXEC mode command displays entries in the ARP table.

Syntax

show arp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds
```

```
Interface        IP address       HW address       Status

---------        ----------       --------------   -------
                                  ---

g1               10.7.1.102       00:10:B5:04:DB   Dynamic
                                  :4B

g2               10.7.1.135       00:50:22:00:2A   Static
                                  :A4
```

ip domain-name

The **ip domain-name** Global Configuration mode command defines a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). To remove the default domain name, use the **no** form of this command.

Syntax

ip domain-name *name*

no ip domain-name

Parameters

- *name* — Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-158 characters)

Default Configuration

A default domain name is not defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines default domain name www.3Com.com.

```
Console(config)# ip domain-name www.3Com.com
```

ip name-server

The **ip name-server** Global Configuration mode command defines the available name servers. To remove a name server, use the **no** form of this command.

Syntax

ip name-server *server-address* [*server-address2 … server-address8]*

no ip name-server [*server-address1 … server-address8*]

Parameters

- *server-address* — Specifies IP addresses of the name server.

Default Configuration

No name server addresses are specified.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

Example

The following example sets the available name server.

```
Console(config)# ip name-server 176.16.1.18
```

21 MANAGEMENT ACL COMMANDS

management access-list

The **management access-list** Global Configuration mode command configures a management access list and enters the Management Access-list Configuration command mode. To delete an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

Parameters

- *name* — Access list name. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. The command enters the Access-list Configuration mode, where permit and deny access rules are defined using the **permit (Management)** and **deny (Management)** commands.

If no match criteria are defined, the default is deny.

If you reenter an access list context, the new rules are entered at the end of the access list.

Use the **management access-class** command to select the active access list.

The active management list cannot be updated or removed.

Management ACL requires a valid management interface, which is a port, VLAN, or port-channnel with an IP address or console interface. Management ACL only restricts access to the device for management configuration or viewing.

Example

The following example creates a management access list called 'mlist', configures management Ethernet interfaces g1 and g9 and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# permit ethernet 1g
Console(config-macl)# permit ethernet g9
Console(config-macl)# exit
Console(config)# management access-class mlist
```

The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except Ethernet interfaces g1 and g9 and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# deny ethernet g1
Console(config-macl)# deny ethernet g9
Console(config-macl)# permit
Console(config-macl)# exit
Console(config)# management access-class mlist
```

permit (Management)

The **permit** Management Access-List Configuration mode command defines a permit rule.

Syntax

permit [**ethernet** interface-number | **vlan** vlan-id | **port-channel** port-channel-number |] [**service** service]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number* |] [**service** *service*]

Parameters

- *interface-number* — A valid Ethernet port number.

- *vlan-id* — A valid VLAN number.
- *port-channel-number* — A valid port channel index.
- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- *prefix-length* — Number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- *service* — Service type. Possible values: **telnet**, **ssh**, **http**, **https** and **snmp**.

Default Configuration

If no permit rule is defined, the default is set to deny.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following example permits all ports in the access list called ‘mlist’.

```
Console(config)# management access-list mlist
Console(config-macl)# permit
```

deny (Management)

The **deny** Management Access-List Configuration mode command defines a deny rule.

Syntax

deny [**ethernet** interface-number | **vlan** vlan-id | **port-channel** port-channel-number |] [**service** service]

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number* |] [**service** *service*]

Parameters

- *interface*-number — A valid Ethernet port number.
- *vlan-id* — A valid VLAN number.
- *port-channel-number* — A valid port-channel number.
- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- *service* — Service type. Possible values: **telnet**, **ssh**, **http**, **https** and **snmp**.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following example denies all ports in the access list called ‘mlist’.

```
Console(config)# management access-list mlist
Console(config-macl)# deny
```

management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. To disable this restriction, use the **no** form of this command.

Syntax

management access-class {c**onsole-only** | *name*}

no management access-class

Parameters

- **console-only** — Indicates that the device can be managed only from the console.
- *name* — Specifies the name of the access list to be used. (Range: 1-32 characters)

Default Configuration

If no access list is specified, an empty access list is used.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an access list called ‘mlist’ as the management access list.

```
Console(config)# management access-class mlist
```

show management access-list

The s**how management access-list** Privileged EXEC mode command displays management access lists.

Syntax

show management access-list [*name*]

Parameters

- *name* — Specifies the name of a management access list. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the ‘mlist’ management access list.

```
Console# show management access-list mlist
mlist
-----
                                  permit ethernet g1
                                  permit ethernet g2
! (Note: all other access implicitly denied)
```

show management access-class

The **show management access-class** Privileged EXEC mode command displays the active management access list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the active management access list.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

22 WIRELESS ROGUE AP COMMANDS

rogue-detect enable (Radio)

The **rogue-detect enable** AP Interface Radio Configuration mode command enables detection of rogue APs. To disable rouge APs detection, use the **no** form of this command.

Syntax

rogue-detect enable

no rogue-detect enable

Parameters

This command has no keywords or arguments.

Default Configuration

Rogue detection is disabled.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

Use the **rogue-detect enable** Global Configuration command to globally enable/disable rogue detection. Rouge detection can be enabled on a specific AP only if rogue detection is enabled globally and for the AP.

Example

The following example enables the detection of rogue APs.

```
Console (Config-wlan-ap)# enterprise config
Console (Config-ap)# interface radio 802.11g
Console (Config-ap-radio-if)# rogue-detect enable
```

rogue-detect rogue-scan-interval

The **rogue-detect rogue-scan-interval** AP Interface Radio Configuration mode command defines the scanning interval for rogue APs. To restore defaults, use the **no** form of this command.

Syntax

rogue-detect rogue-scan-interval {**long** | **medium** | **short**}

no rogue-detect rogue-scan-interval

Parameters

- **long** — Scanning interval of 240 seconds.
- **medium** — Scanning interval of 150 seconds.
- **short** — Scanning interval of 20 seconds.

Default Configuration

The default scanning interval is long.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

A long scanning interval causes the least disruption of user traffic performance, while a short scanning interval causes the most disruption of user traffic performance.

Example

The following example defines the scanning interval for rogue APs at 150 seconds.

```
Console (Config-ap)# interface radio 802.11g
Console (Config-ap-radio-if)# rogue-detect rogue-scan-interval medium
```

wlan rogue-detect rogue-ap

The **wlan rogue-detect rogue-ap** Global Configuration mode command sets the status of rouge APs. To restore defaults, use the **no** form of this command.

Syntax

wlan rogue-detect rogue-ap *mac-address* **state** {**known** | **mitigate**}

no wlan rogue-detect rogue-ap *mac-address* **state**

Parameters

- *mac-address* — The rogue AP MAC address.
- **known** — Specify that the rogue AP is known.
- **mitigate** — Specify that the rogue AP should be mitigated.

Default Configuration

New.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the status of rogue AP with the MAC address 00-9E-92-4C-73-FCas known.

```
Console (config-ap)# wlan rogue-detect rogue-ap
00-9E-92-4C-73-FC state known
```

clear wlan rogue-ap

The **clear wlan rogue-ap** Privileged EXEC mode command deletes a rogue AP from the rogue APs list.

Syntax

clear wlan rogue-ap *mac-address*

Parameters

- *mac-address* — The rogue AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Deleting a rogue AP from the list does not mitigate or suppress the rogue. If the rogue AP is still physically present and active, it will reappear in the Rogue Access Point list after subsequent scans for rogue APs is performed.

Example

The following example deletes a rogue AP with the MAC address 00-9E-92-4C-73-FC from the rogue APs list.

```
Console# clear wlan rogue-ap 00-9E-92-4C-73-FC
```

show wlan rogue-aps configuration

The **show wlan rogueaps configuration** Privileged EXEC mode command displays information about rogue APs detection configuration.

Syntax

show wlan rogue-aps configuration [*name* | *mac-address*]

Parameters

- *name* — Specify the AP name. (Range: 1-32 characters)
- *mac-address* — Specify the AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about rogue APs detection configuration.

```
Console# show wlan rogue-aps configuration


Rogue APs detection is enabled.


AP name          Radio            Scanning         Interval
-----------      --------         --------         -------------
AP1              a                Enabled          Long
AP1              g                Enabled          Long
AP2              a                Enabled          Long
AP2              g                Enabled          Long
```

show wlan rogue-aps list

The **show wlan rogue-aps list** Privileged EXEC mode command displays information about potential rogue APs.

Syntax

show wlan rogue-aps list [**mac** *mac-address*]

Parameters

- *mac-address* — The rogue AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The show wlan rogue-aps list command displays each rogue at one entry, even if it was discovered by more than one Radio.

Example

The following example displays information about potential rogue APs.

```
Console# show wlan rogue-aps list


MAC           Status        SSID          Ch            Last seen
Address

----------    ------        ----          --            ---------
-

WlanSys-82    New           test          1             3-Aug-2005
-73-FC                                                  15:41:43

WlanSys-82    Known         c1            3             3-Aug-2005
-78-FC                                                  15:48:12

WlanSys-82    Mitigated                   3             3-Aug-2005
-79-FC                                                  19:32:42
```

show wlan rogue-aps neighborhood

The **show wlan rogue-aps neighborhood** Privileged EXEC mode command displays a list of APs that have detected a rogue AP.

Syntax

show wlan rogue-aps neighborhood mac-address

Parameters

- mac-address — The AP MAC address detecting rogue APs.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays a list of APs that has detected a rogue AP with the MAC address:

00-9E-93-82-73-FC.

```
Console# show wlan rogue-aps neighborhood 00-9E-93-82-73-FC


AP name                           Signal [dBm]
-----------                       -------------------
AP1                               -62
AP2                               -68
Lobby                             -68
```

23 WIRELESS ESS COMMANDS

wlan ess create

The **wlan ess create** Global Configuration mode command creates an ESS. To remove the ESS, use the **no** form of this command.

Syntax

wlan ess create *index ssid*

no wlan ess create index

Parameters

- *index* — The ESS index. (Range: 2-65535)
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

ESS number 1 always exists.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example creates an ESS with the index of 1200 and the SSID of ‘abc123’.

```
Console (config)# wlan ess create 1200 abc123
```

wlan ess configure

The **wlan ess configure** Global Configuration mode command enters the ESS Configuration mode.

Syntax

wlan ess configure {**id** *index* | **ssid** *ssid*}

Parameters

- *index* — The ESS index. (Range: 1-65535)
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the ESS ‘enterprise’ configuration mode.

```
Console (Config)# wlan ess configure id 1200
Console (Config-ess)#
```

ssid

The **ssid** ESS Configuration mode command configures the SSID name of an ESS.

Syntax

ssid *ssid*

Parameters

- *ssid* — The SSID string of the ESS name. (Range:1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

ESS Configuration mode

User Guidelines

The SSID string must be a unique string in the system. The command fails if there already exists an SSID with the same name.

Example

The following example configures the SSID name of an ESS as ‘enterprise’.

```
Console (config)# ssid enterprise
Console (config)# wlan ess configure ssid enterprise
```

open vlan

The **open vlan** ESS Configuration mode command configures the ESS VLAN when there is no security suite for the ESS. To restore defaults, use the **no** form of this command.

Syntax

open vlan *vlan-id*

no open vlan

Parameters

- *vlan-id* — VLAN ID of the ESS default VLAN.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

VLAN number 1.

Command Mode

ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the ESS VLAN when there is no security suite for the ESS to VLAN ID number 2.

```
Console (Config)# wlan ess configure ssid enterprise
Console (Config-ess)# open vlan 2
```

qos

The **qos** ESS Configuration mode command enables QoS in an ESS. To disable QoS, use the no form of this command.

Syntax

qos {*wmm* | *svp*}

no qos

Parameters

- *wmm* — Wi-Fi WMM mode.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

QoS in an ESS is disabled.

Command Mode

ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables QoS in an ESS in the Wi-Fi WMM mode.

```
Console (Config)# wlan ess configure ssid enterprise
Console (Config-ess)# qos wwm
```

load-balancing

The **load-balancing** ESS Configuration mode command enables load balancing in an ESS. To disable load balancing, use the no form of this command.

Syntax

load-balancing {**association** | **periodically**} no load-balancing

Parameters

- *association* — Load balancing calculations are performed when a station attempts to associate with an AP in the ESS. The associating station can be moved to an adjacent AP in the ESS prior to association.
- *periodically* — Load balancing calculations are performed at a fixed interval for all APs in an ESS. Stations are moved to suitable APs in the ESS based on load balancing calculations.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

Disabled.

Command Mode

ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables load balancing in an ESS where a station attempts to associate with an AP in the ESS.

```
Console (Config)# wlan ess configure ssid enterprise
Console (Config-ess)# load-balancing association
```

mac-filtering action

The **mac-filtering action** ESS Configuration mode command enables source MAC address filtering in an ESS. To disable source MAC address filtering, use the **no** form of this command.

Syntax

mac-filtering action {permit | deny}

no mac-filtering action

Parameters

- *permit* — Permit only stations where their MAC address is in the MAC-address-filtering list.

- *deny* — Deny stations where their MAC address is in the MAC-address-filtering list.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

Disabled.

Command Mode

ESS Configuration mode

User Guidelines

- The decision to allow a station to access the ESS is done only during the association time.
- Use the mac-filtering list command to configure the MAC-address-filtering list.

Example

The following example denies source MAC-address filtering in an ESS.

```
Console (Config)# wlan ess configure ssid enterprise
Console (Config-wlan-ess)# mac-filtering action deny
```

mac-filtering list

The **mac-filtering list** ESS Configuration mode command adds and removes MAC addresses from the MAC address filtering list in an ESS. To delete all the MAC addresses, use the **no** form of this command.

Syntax

mac-filtering list {**add** | **remove**} *mac-address*

no mac-filtering list

Parameters

- **add** — Adds the defined MAC addresses to the MAC address filtering list in an ESS.
- **remove** — Removes the defined MAC addresses from the MAC address filtering list in an ESS.
- *mac-address* — A valid MAC address.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

Empty list.

Command Mode

ESS Configuration mode

User Guidelines

Use the mac-filtering action ESS configuration command to enable the MAC-address-filtering list and to define the MAC-address-filtering list type.

Example

The following example adds the MAC address 00-9E-92-4C-73-FC to the MAC address filtering list in an ESS.

```
Console (Config)# wlan ess configure ssid enterprise
Console (Config-wlan-ess)# mac-filtering list add
00-9E-92-4C-73-FC
```

security suite create

The **security suite create** ESS Configuration command creates a security suite for an ESS. To delete a security suite, use the **no** form of this command.

Syntax

security suite create *type* [{**key-hex** | **key-ascii**} *encryption-key*]

no security suite create *type*

Parameters

- *type* — The security suite type. Available values are as follows:
  - *open-wep* — No authentication with WEP for data encryption. Wired Equivalent Privacy (WEP) is a scheme to secure wireless networks (WiFi). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP provides comparable confidentiality to a traditional wired network. WEP provides a bare minimal level of security that can deter casual snooping.
  - *shared-wep* — Shared authentication only with WEP encryption.
  - *open-shared-wep* — Open or shared authentication with WEP encryption.

  - *802.1x* — 802.1x authentication with WEP.
  - *wpa* — Wi-Fi Protected Access (WPA and WPA2) are systems to secure wireless (Wi-Fi) networks. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards.
  - *wpa-psk* — WPA with pre-shared key.
  - *wpa2* — Indicates that Wi-Fi Protected Access 2 (WPA) is the selected WLAN security method. WPA2 with 802.1x authenticates WLAN users and dynamically generate keys.
  - *wpa2-psk* — WPA2 with pre-shared key.
- **key** — A key must be entered for **open-wep**, **shared-wep**, **openshared-wep**, **wpa-psk** and **wpa2-psk**. A key should not be entered for **802.1x**, **wpa** and **wpa2**. See the **key** command in Security-Suite ESS Configuration mode for information on the range of the key size.
  - *key-hex* — Specifies the entry of a pre-shared key (psk) in hexadecimal format. (Range: 10-26 characters)
  - *key-ascii* — Specifies the entry of a pre-shared key (psk) in ASCII format. (Key length: 5 or 13 characters)
- *encryption-key* — Specifies the pre-shared key. See usage guidelines for the key size range.
- *ssid* — The ESS SSID string. (Range: 1-32 characters)

Default Configuration

WPA security suite exists.

Command Mode

ESS Configuration mode

User Guidelines

- If no security-suite exists, the product works in 802.11 open security mode.
- WPA security suite and WPA-PSK security suite cannot exist simultaneously.

- WPA2 security suite and WPA2-PSK security suite cannot exist simultaneously.
- At one time, only one security-suite per ESS can exist.
- Open-WEP security suite and WEP security suite cannot exist simultaneously.
- For Open-WEP and WEP keys you should enter one of the following options: 40 bits or 104 bits.
- For WPA-PSK and WPA2-PSK keys you should enter 8 – 63 ASCII chars (It is recommended to enter at least 20 chars), or 256 bits in hex format.

Example

The following example creates a security suite for an ESS.

```
Console (Config)# wlan ess configuressid enterprise
Console (Config-wlan-ess)# security suite create open-wep
```

security suite configure

The s**ecurity suite configure** ESS Configuration mode command enters the Security-Suite Configuration mode.

Syntax

security suite configure *type*

Parameters

- *type* — The security suite type. Available values are as follows:
  - **open-wep** — No authentication with WEP for data encryption. Wired Equivalent Privacy (WEP) is a scheme to secure wireless networks (WiFi). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP provides comparable confidentiality to a traditional wired network. WEP provides a bare minimal level of security that can deter casual snooping.
  - *shared-wep* — Shared authentication only with WEP encryption.
  - *open-shared-wep* — Open or shared authentication with WEP encryption.
  - *802.1x* — 802.1x authentication with WEP.

- *wpa* — Wi-Fi Protected Access (WPA and WPA2) are systems to secure wireless (Wi-Fi) networks. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards.
- *wpa-psk* — WPA with pre-shared key.
- wpa2 — WPA2 method only.
- wpa2-psk — WPA2 with pre-shared key.

Default Configuration

WPA security suite exists.

Command Mode

ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the Security-Suite Configuration mode.

```
Console (Config-wlan-ess)# security suite configure wpa
Console (Config-ess-security)#
```

vlan (Security-Suite ESS)

The **vlan** Security-Suite ESS Configuration mode command configures the policy VLAN for a security-suite. To restore the default configuration, use the **no** form of this command.

Syntax

vlan *vlan-id*

no vlan

Parameters

- *vlan-id* — VLAN ID of the ESS default VLAN.

Default Configuration

VLAN #1

Command Mode

Security-Suite ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the policy VLAN for a security-suite to VLAN ID 5.

```
Console (Config-wlan-ess)# security suite configure wpa
Console (Config-ess-security)# vlan 5
```

timer (Security-Suite ESS)

The **timer Security-Suite** ESS Configuration mode command configures the key exchange timers for a Security-Suite. To restore the default configuration, use the **no** form of this command.

Syntax

timer rekey-time-unicast {**never** | *minutes*}

no timer rekey-time-unicast

timer rekey-time-multicast {**never** | *minutes*}

no timer rekey-time-multicast

timer reauth-time {**never** | *seconds*}

no timer reauth-time

timer idle-time {**never** | *seconds*}

no timer idle-time

Parameters

- **rekey-time-unicast** *minutes* — Unicast rekeying timeout period. (Range: 1-4294967295)
- **rekey-time-multicast** *minutes* — Multicast rekeying timeout period. (Range: 1-4294967295)

- **reauth-time** *seconds* — Re-authentication timeout period. (Range: 1-4294967295)
- **idle-time** *seconds* — DLE timeout period. (Range: 1-9676800)
- **never** — There is an unlimited rekeying timeout period.

Default Configuration

- **rekey-time-unicast** — Never
- **rekey-time-multicast** — Never
- **reauth-time** — 14400
- **idle-time** — Never

Command Mode

Security-Suite ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the key exchange timers for a security-suite as an unlimited rekeying timeout period.

```
Console (Conf\ig-wlan-ess)# security suite configure wpa
Console (Config-ess-security)# timer rekey-time-unicast never
```

update-gkey-on-leave (Security-Suite ESS)

The **update-gkey-on-leave** Security-Suite ESS Configuration mode command defines that a group key should be updated after a station leaves the AP. To disable updates, use the **no** form of this command.

Syntax

update-gkey-on-leave

no update-gkey-on-leave

Parameters

This command has no keywords or arguments.

Default Configuration

No key is defined.

Command Mode

Security-Suite ESS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines that a group key should be updated after a station leaves the AP.

```
Console (Config-wlan-ess)# security suite configure wpa
Console (Config-ess-security)# update-gkey-on-leave
```

wpa2 pre-authentication

The **wpa2 pre-authentication** ESS Configuration mode command enables WPA2 pre-authentication in an ESS. Use the wpa2 pre-authentication command in ESS Configuration mode. To disable WPA2 pre-authentication, use the **no** form of this command.

Syntax

wpa2 pre-authentication

no wpa2 pre-authentication

Parameters

This command has no keywords or arguments.

Default Configuration

This command has no default configuration.

Command Mode

ESS Configuration mode

User Guidelines

The command can only be enabled if WPA2 PMK caching is enabled.

Example

The following example enables WPA2 pre-authentication in an ESS.

```
Console (Config-wlan-ess)# configure ssid enterprise
Console (Config-ess-security)# wpa2 pre-authentication
```

show wlan ess

The **show wlan** Privileged EXEC mode command displays information on the ESS configuration.

Syntax

show wlan ess configuration [**id** *1-65535* | **ssid** *1-32*]

show wlan ess vlans [**id** *1-65535* | **ssid** *1-32*]

show wlan ess radios [**id** *1-65535* | **ssid** *1-32*]

Parameters

- *index* — The ESS index. (Range: 1-65535)
- *ssid* — The SSID string of the ESS. (Range: 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the display of the WLAN ESS configuration.

```
console # show wlan ess configuration


Index     SSID      Securit   Load      QoS       MAC Filter
                    y Suite   Bal.

-----     ----      -------   -------   ---       ------
                    -         --

1         Enterpr   WPA,      Assoc.    WMM       Dis
          ise       WPA2

2         Guest     Open      Dis       Dis       Permit
```

The following example configures the display of the defined ESS configurations.

```
Console # show wlan ess configuration 1

Index: 1
SSID: Enterprise
Load Balancing: Association
QoS: WMM
Mac Filter: Disabled
WPA2 Preauthentication: Enabled
Open VLAN: 1

Security Suite:  WPA
VLAN: 8
Unicast Rekeying Timeout: Never
Multicast Rekeying Timeout: Never
Update Group Key On Leave: Enabled

Security Suite:  WPA2
VLAN: 9
Unicast Rekeying Timeout: Never
Multicast Rekeying Timeout: Never
Update Group Key On Leave: Enabled

Console # show wlan ess configuration 2

Index: 2
SSID: Guest
Load Balancing: Disabled
QoS: Disabled
Mac Filter: Permit
WPA2 Preauthentication: Enabled
Open VLAN: 1

Security suite: WPA
VLAN: 1
Unicast Rekeying Timeout: 0
Multicast Rekeying Timeout: 0
Update Group Key On Leave: Enabled
```

The following example configures the display of WLAN ESS radios' configuration.

```
Console # show wlan ess radios


Index                SSID                 Radios
-----                -----                ------
1                    Enterprise           AP1(a), AP1(g),
                                          AP2(a), AP2(g),
                                          AP3(a), AP3(g)
2                    Guest                AP1(g), AP2(g)
```

show wlan ess mac-filtering lists

The **show wlan** Privileged EXEC mode command displays the ESS MAC filtering lists.

Syntax

show wlan ess mac-filtering lists {**id** *index* | **ssid** *ssid*}

Parameters

- *index* — The ESS index. (Range: 1-65535)
- *ssid* — The SSID string of the ESS. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the ESS MAC filtering lists.

```
Console # show wlan ess mac-filtering lists guest

Action: Permit

00-9E-93-82-83-A1
00-9E-93-82-83-A2
00-9E-93-82-83-A3
```

show wlan ess counters

The **show wlan ess counters** Privileged EXEC mode command displays the number of stations at each ESS.

Syntax

show wlan ess counters [*index* | *ssid*]

Parameters

- *index* — The ESS index. (Range: 1-65535)
- *ssid* — The SSID string of the ESS. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays station numbers at each ESS.

```
Console# show wlan ess counters

Index                 SSID                  Stations
-----                 ----                  -------
1                     Enterprise            182
2                     Guest                 3
```

The following example displays station numbers at ESS ‘enterprise’.

```
Console# show wlan ess counters ssid enterprise

AP                    Radio                 Stations
--                    ----                  --------
AP1                   a                     32
AP1                   g                     29
AP2                   a                     12
AP2                   g                     42
AP3                   a                     31
```

24 WIRELESS AP GENERAL COMMANDS

clear wlan ap

The **clear wlan ap** Privileged EXEC mode command deactivates an AP.

Syntax

clear wlan ap {*name* | *mac-address*}

Parameters

- *name* — The AP name. (Range: 1-32 characters)
- *mac-address* — The AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- When the configurations of all the deactivated AP is deleted, the AP may reappear in the AP Discovery Table.
- The **clear wlan ap** command can also be used to remove an AP that is irrelevant (either associated with another device or removed from the system) from the APs discovery table. If the AP is still relevant (not associated with another device and not removed from the system), it should not be removed from the discovery table.

Example

The following example deactivates an AP called enterprise.

```
Console (config)# clear wlan ap enterprise
```

wlan ap active

The **wlan ap active** Global Configuration mode command activates an AP.

Syntax

wlan ap active *mac-address* [**template** *template-name*]

Parameters

- *mac-address* — MAC address of the AP to be activated.
- *template-name* — Specify a template AP to be used. If unspecified the device defaults to the AP default parameters .(Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example activates an AP with the MAC address 00:0e:35:63:5c:a7.

```
Console (Config)# wlan ap active 00:0e:35:63:5c:a7
```

wlan ap key

The **wlan ap key** Global Configuration mode command configures a secure key for communication to an AP. To remove an AP, use the **no** form of the command.

Syntax

wlan ap {*name* | *mac-address*} **key** {**hex** *hex-number* | **ascii** *string*}

no wlan ap {*name* | *mac-address*} **key**

Parameters

- *name* — The AP name. The AP name can be specified only for active APs. (Range: 1-16 characters)

- *mac-address* — The AP MAC address.
- **hex** *hex-number* — The secure key in hexadecimal format. 32 hexadecimal characters must be entered.
- **ascii** *string* — The secure key in hexadecimal format. From 1-16 characters can be entered. If less than 16 characters are entered, the software completes the key to 16 characters with blank characters.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

If the secure key is not set before activation at the AP, that key would be transferred to the AP on activation.

A key cannot be removed in an active AP.

Example

The following example configures a secure key for communication to an AP called ‘enterprise’.

```
Console (config)# wlan ap enterprise key ascii 1234567
```

wlan ap config

The **wlan ap config** Global Configuration mode command sets the device in AP Configuration mode.

Syntax

wlan ap {*name* | *mac-address*} **config**

Parameters

- *name* — The AP name. (Range: 1-32 characters)
- *mac-address* — The AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Only active APs can be placed in AP Configuration mode.

Example

The following example sets the device in AP Configuration mode.

```
Console (Config)# wlan ap CR1 config
Console (Config-wlan-ap)#
```

name

The **name** AP Configuration mode command configures a wireless AP name. To restore the default configuration, use the **no** form of this command.

Syntax

name string

no name

Parameters

- *name* — The AP name.

Default Configuration

The AP's MAC address.

Command Mode

AP Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures a wireless AP name to 'enterprise' .

```
Console (Config)# wlan ap CR1 config
Console (Config-ap)# name enterprise
```

tunnel priority

The **tunnel priority** AP Configuration mode command configures a wireless AP priority for VLAN tunneling. To restore default settings, use the **no** form of this command.

Syntax

tunnel priority *priority*

no priority

Parameters

- *priority* — The relative priority of the wireless AP as a source for VLANs. The number 0 indicates that the AP cannot be a source for VLANs. (Range: 0-99)

Default Configuration

The default wireless AP priority for VLAN tunneling is 20.

Command Mode

AP Configuration mode

User Guidelines

If one of the stations that are associated with an AP is associated with a VLAN that the AP does not have a direct connection to, the AP initiates a tunnel with the AP that has a direct connection to that VLAN. The AP with the highest tunneling priority in the network is chosen as the source of the VLAN.

Example

The following example configures a wireless AP priority for VLAN tunneling to 30.

```
Console (Config)# wlan ap CR1 config
Console (Config-ap)# tunnel priority 30
```

wan enable

The **wan enable** AP configuration mode command accommodates certain timing constrains in the communication to a remotely connected wireless AP separated by a WAN link or the Internet. To disable WAN support, use the **no** form of this command.

Syntax

wan enable

no wan enable

Parameters

This command has no keywords or arguments.

Default Configuration

Disabled

Command Mode

AP Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example accommodates certain timing constrains in the communication to a remotely connected wireless AP separated by a WAN link or the Internet.

```
Console (Config)# wlan ap CR1 config
Console (Config-ap)# wan enable
```

interface ethernet

The **enter interface** AP Configuration mode command configures an interface and enters the Interface Configuration mode.

Syntax

interface ethernet

Parameters

This command has no keywords or arguments.

Default Configuration

This command has no default configuration.

Command Mode

AP Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the Interface Configuration mode.

```
Console (Config-ap)# interface ethernet
Console (Config-ap-if)#
```

vlan allowed

The **vlan allowed AP** interface Ethernet Configuration mode command adds or removes VLANs to the Ethernet port of a wireless AP. To restore the default configuration, use the **no** form of this command.

Syntax

vlan allowed {**add** *vlan-list* | **remove** *vlan-list*}

no vlan allowed

Parameters

- **add** *vlan-list* — List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **remove** *vlan-list* — List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

Default Configuration

VLAN number 1.

Command Mode

AP interface Ethernet Configuration mode

User Guidelines

A VLAN cannot be removed from the allowed VLANs if it is defined as a native VLAN.

Example

The following example adds VLANs 1,2,3 and 4 to the Ethernet port of a wireless AP.

```
Console (Config-ap)# interface ethernet
Console (Config-ap-if)# vlan allowed add 1-4
```

vlan native

The **vlan native** AP interface Ethernet Configuration mode command sets the native VLAN of the Ethernet port of a wireless AP. To restore the default configuration, use the **no** form of this command.

Syntax

vlan native *vlan-id*

no vlan native

Parameters

- *vlan-id* — VLAN ID of the native VLAN.

Default Configuration

VLAN #1

Command Mode

AP interface Ethernet Configuration mode

User Guidelines

A VLAN can be defined as a native VLAN only if it is **one** of the allowed VLANs.

Example

The following example sets the native VLAN of the Ethernet port for a wireless AP to 2.

```
Console (Config-ap)# interface ethernet
Console (Config-ap-if)# vlan native 2
```

wlan template ap configure

The wlan template ap configure Global Configuration mode command places the device in wireless AP Template Configuration mode.

Syntax

wlan template ap configure name

Parameters

- name — The name of the AP template. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

All AP configuration commands are relevant to template APs, except for the name AP configuration command and wlan ap key Global Configuration commands.

Example

The following example places the device in wireless AP template configuration mode to configure template called ‘type1’.

```
Console (Config)# wlan template ap configure type1
Console (Config-wlan-template-ap)#
```

set wlan copy

The **set wlan copy** wireless AP template configuration command copies the wireless AP configuration parameters from the template AP to an AP.

Syntax

set wlan copy ap {**default** | *template-nam*e} **to ap** *ap-name*

set wlan copy ap *ap-name* **to template ap** {*template-name*}

Parameters

- **default** — The default template.
- *template-name* — The template AP name. (Range: 1 – 32 characters)
- *ap-name* — The AP name. (Range: 1 – 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Wireless AP template configuration mode

User Guidelines

Copying the template to an AP overrides the entire AP configuration with the template configuration.

Example

The following example copies a wirless AP configuration parameters from a template AP “enterprise” to an AP called “Switch”.

```
Console (Config)# wlan template ap configure type1
Console (Config-wlan-template-ap)# set wlan copy ap enterprise
to ap Switch
```

show wlan aps

The **show wlan aps** Privileged EXEC mode command displays information on active APs.

Syntax

show wlan aps [*name* | *mac-address*]

show wlan aps radio [*a* | *g*]

show wlan aps *ess* [*ssid*]

show wlan aps vlans [*ssid*]

show wlan aps version [*name* | *mac-address*]

Parameters

- ***name*** — The AP name. (Range: 1-32 characters)
- *mac-address* — The AP MAC address.
- **a** — Radio type is 802.1a.
- **g** — Radio type is 802.1g.
- *ssid* — The ESS SSID. (Range: 1-32 characters)

Default Configuration

- name
- ssid

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on active APs.

```
Console # show wlan aps


Name            MAC Address        Type             State

------          ---------------    ------           --------

AP1             00-9E-92-4C-73-    a, g             Enabled
                FC

AP2             00-9E-92-4C-73-    a, g             Disabled
                FD
```

The following example displays detailed information on a specific active AP:

```
Console # show wlan aps AP1


Name: AP1
MAC Address: 00-9E-92-4C-73-FC
Type: a, g
State: Enabled
Status: Disabled
802.11a Radio: Enabled
802.11g Radio: Enabled
VLANs Allowed: 2, 3
Native VLAN: 2
Tunnel Priority: 20
IP address: 172.16.1.1
DNS name: wlan-switch1.ge.com
WAN Timing Constrains: Disabled
Console Logging: Disabled
```

The following example displays important radio information on all the active APs.

```
Console # show wlan aps radio


Name     Radio    State    Power    Channel  Traffic  Allow
                                             Oper     Admin

-------  -------  -------  -------  -------  -------  -------
         -        -        -        ----     -------  -------
                                             -------  -------

AP1      a        Enabled  Maximum  LG       Enabled  N/A
AP1      g        Enabled  Maximum  LG       Enabled  Enabled
AP2      a        Enabled  Maximum  44       Enabled  N/A
AP2      g        Enabled  Maximum  11       Enabled  Enabled
```

The following example displays the SSIDs that are associated with each active AP.

```
Console # show wlan aps ess


Name          Radio         SSID          State         Advertise

------        --------      ------        --------      -----------
                                                        --

AP1           a             Enterprise    Enabled       Enabled

AP1           a             Guest         Enabled       Enabled

AP2           g             Enterprise    Enabled       Enabled

AP2           a             Guest         Enabled       Enabled
```

The following example displays:

1) Station VLANs: List all the VLANs required for the stations that are associated with that AP.

2) Ethernet VLANs: The VLANs configured on the AP Ethernet port.

3) Priority: The priority of the AP as a source for tunneling.

```
Console # show wlan aps vlans


Name            Station VLANs    Ethernet VLANs   Priority

------          --------------   --------------   -------------
                ------           --------

AP1             1, 2, 3             1, 2          30

AP2             1, 2, 3, 4       1, 3, 4          20
```

The following example displays the AP model, serial number and software versions.

```
Console # show wlan aps versions


Name         Model        Serial       Boot Loader  Software
                          number       Version      Version

-------      --------     -----------  -----------  -----------
                          ---------    -----------  -----------
                                       --------     ----

AP1          A1           3987587439   1.1.0.1      1.2.71 (d)

AP2          A1           398758638    1.1.0.1      1.2.71 (d)
                          7
```

show wlan ap interface radio

The **show wlan ap interface radio** Privileged EXEC mode command displays information on an AP radio interface.

Syntax

show wlan ap {*name* | *mac-address*} **interface radio** {**a** | **g**} [**ess ssid**]

Parameters

- *name* — The AP name.
- *mac-address* — The AP MAC address.
- **a** — Radio type is 802.1a.
- **g** — Radio type is 802.1g.
- *ssid* — The ESS SSID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on an AP radio interface.

```
Console # show wlan ap AP1 interface radio g
State: Enabled
Allow traffic: Enabled
Channel: Least Congested (11).
Power: Maximum
Allow 802.11b: Enabled
Preamble: Long
RTS Threshold: 2312 bytes
Antenna: Diversity
Beacon Period: 100 ms
```

```
SSID          BSSID        Advertise      Data Rates
------        --------     -------------- ----------------
Enterprise    Enabled      Enabled        6(m), 9, 12, 18, 24, 36, 48, 54
Guest         Enabled      Enabled        1(m), 2, 5.5, 6, 9, 11, 12, 18, 24
```

show wlan ap interface ethernet

The s**how wlan ap interface ethernet** Privileged EXEC mode command displays information on an AP radio interface.

Syntax

show wlan ap {*name* | *mac-address*} **interface ethernet**

Parameters

- *name* — The AP name.
- *mac-address* — The AP MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on an AP radio interface.

```
Console # show wlan ap AP1 interface ethernet

VLANs Allowed: 2, 3
Native VLAN: 2
Tunnel source: Enabled
Tunnel priority: 20
Ethernet MAC address: 00-9E-92-8C-73-FC
```

show wlan aps counters

The **show wlan aps counters** Privileged EXEC mode command displays information on the AP traffic.

Syntax

show wlan aps counters [**radio a** | **g**] [**ap** *name*]

Parameters

- **radio a** | b — Specified Radio type. If unspecified shows the total traffic on the AP.
- **ap** *name* — Specified AP name. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on the AP traffic.

```
Console# show wlan aps counters


Name          Stations      Name          Stations

------        -----------   ------        -----------
              --                          --

AP1           19            AP1           19

AP2           23            AP2           23


Name          InUcastPk     InPkts        InOctets      In Errors
              ts

------        -----------   ----------    -----------   -----------
              --                          ------        ---

AP1           756857        8691          8432          2

AP2           846584        9132          8921          2


Name          InUcastPk     InPkts        InOctets      In Errors
              ts

------        -----------   ----------    -----------   -----------
              --                          ------        ---

AP1           756857        8691          8432          2

AP2           846584        9132          8921          2


Name          OutUcastP     OutPkts       OutOctets     Out Errors
              kts

------        ---------     ----------    --------      -------

AP1           87398238      922982        8118710       2

AP2           846584        913287        783278        2
```

```
Console# show wlan aps counters ap AP1

Number of stations: 19

In Octets: 756857
In Packets: 8691
In Unicast Packets: 8432
In Data Packets: 8533
In Management Packets: 158
In Errors: 2

Out Octets: 87398238
Out Packets: 922982
Out Unicast Packets: 811871
Out Data Packets: 881831
Out Management Packets: 41151
Out Errors: 0
```

show wlan aps discovered

The **show wlan aps discovered** Privileged EXEC mode command displays wireless APs that were discovered but not activated.

Syntax

show wlan aps discovered [*mac-address*]

Parameters

- *mac-address* — MAC address of the AP.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays wireless APs that were discovered but were not activated.

```
Console # show wlan aps discovered


MAC Address      Key              Discovery Time   Status

--------------                    --------------   ----------
---                               --------

00-9E-92-4C-73                    3-Aug-2005       Discovered
-FC                               15:41:43

00-9E-92-4C-73                    3-Aug-2005       Discovered
-FD                               17:19:48
```

show wlan template aps

The **show wlan template aps** Privileged EXEC mode command displays the template AP configuration.

Syntax

s**how wlan template** aps [*name*]

Parameters

- *name* — Specify the AP name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays displays the template AP configuration.

```
Console # show wlan template aps

Name             Radio a          Radio g
-------          --------         --------
default          Enabled          Enabled
indoor           Enabled          Enabled
outdoor          Enabled          Enabled

Console # show wlan aps indoor

NAME: vivi
MAC Address: 00:f0:00:00:06:25
802.11a Radio: Enabled
802.11g Radio: Enabled
Type: a, g
State: Enabled
VLANs Allowed: 2, 3
Native VLAN: 2
Tunnel Source: Enabled
Tunnel Priority: 20
WAN Timing Constraints: Disabled
Console Logging: Disabled

Radio a
--------
State: Enabled
Allow traffic: Enabled
Channel: Least Congested
Power: Max
Preamble: Long
RTS Threshold: 2312
Antenna: Diversity
Beacon Period: 100
```

25 SSH COMMANDS

ip ssh port

The **ip ssh port** Global Configuration mode command specifies the port to be used by the SSH server. To restore the default configuration, use the **no** form of this command.

Syntax

ip ssh port *port-number*

no ip ssh port

Parameters

- *port-number* — Port number for use by the SSH server (Range: 1-65535).

Default Configuration

The default port number is 22.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
Console(config)# ip ssh port 8080
```

ip ssh server

The **ip ssh server** Global Configuration mode command enables the device to be configured from a SSH server. To disable this function, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

Device configuration from a SSH server is disabled.

Command Mode

Global Configuration mode

User Guidelines

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa**, and **crypto key generate rsa** Global Configuration mode commands.

Example

The following example enables configuring the device from a SSH server.

```
Console(config)# ip ssh server
```

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up on another device.

This command may take a considerable period of time to execute.

Example

The following example generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration which is never displayed to the user or backed up on another device.

This command may take a considerable period of time to execute.

Example

The following example generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```

ip ssh pubkey-auth

The **ip ssh pubkey-auth** Global Configuration mode command enables public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

Public Key authentication fo incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent.

Example

The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

No keys are specified.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob
Console(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

user-key

The **user-key** SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. To remove an SSH public key, use the **no** form of this command.

Syntax

user-key *username* {**rsa** | **dsa**}

no user-key *username*

Parameters

- *username* — Specifies the username of the remote SSH client. (Range: 1-48 characters)
- **rsa** — Indicates the RSA key pair.
- **dsa** — Indicates the DSA key pair.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Follow this command with the **key-string** SSH Public Key-String Configuration mode command to specify the key.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

key-string

key-string row *key-string*

Parameters

- **row** — Indicates the SSH public key row by row.
- *key-string* — Specifies the key in UU-encoded DER format; UU-encoded DER format is the same format in the authorized_keys file used by OpenSSH. (Range:0-160)

Default Configuration

No keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the **key-string** SSH Public Key-string Configuration mode command to specify which SSH public key is to be interactively configured next. To complete the command, you must enter a row with no characters.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key row by row. Each row must begin with a **key-string row** command. This command is useful for configuration files.

Example

The following example enters public key strings for SSH public key client **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2
```

show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:

IP address    SSH           Version      Cipher       Auth Code
              username

----------    -----------   ---------    -------      ----------
              -

172.16.0.1    John Brown    2.0 3        DES          HMAC-SHA1
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	Client address
SSH username	User name
Version	SSH version number

Field	Description
Cipher	Encryption type (3DES, Blowfish, RC4)
Auth Code	Authentication Code (HMAC-MD5, HMAC-SHA1)

show crypto key mypubkey

The **show crypto key mypubkey** Privileged EXEC mode command displays the SSH public keys on the device.

Syntax

show crypto key mypubkey [**rsa** | **dsa**]

Parameters

- **rsa** — Indicates the RSA key.
- **dsa** — Indicates the DSA key.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SSH public RSA keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301
87685768
Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt
gfhkjglk
```

show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]

Parameters

- *username* — Specifies the remote SSH client username.
- **bubble-babble** — Fingerprint in Bubble Babble format.
- **hex** — Fingerprint in Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username                          Fingerprint

--------                          -------------------------------
                                  ----------------

bob                               9A:CC:01:C5:78:39:27:86:79:CC:2
                                  3:C5:98:59:F1:86

john                              98:F7:6E:28:F2:79:87:C8:18:F8:8
                                  8:CC:F8:89:87:C8


Console# show crypto key pubkey-chain ssh username bob

Username: bob
```

```
Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241
00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4

Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

26 Web Server Commands

ip http server

The **ip http server** Global Configuration mode command enables configuring the device from a browser. To disable this function, use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

User Guidelines

Only a user with access level 15 can use the Web server.

Example

The following example enables configuring the device from a browser.

```
Console(config)# ip http server
```

ip http port

The **ip http port** Global Configuration mode command specifies the TCP port to be used by the Web browser interface. To restore the default configuration, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

Parameters

- *port-number* — Port number for use by the HTTP server. (Range: 1-65535)

Default Configuration

The default port number is 80.

Command Mode

Global Configuration mode

User Guidelines

Specifying 0 as the port number effectively disables HTTP access to the device.

Example

The following example configures the http port number to 100.

```
Console(config)# ip http port 100
```

ip http exec-timeout

The **ip http exec-timeout** Global Configuration mode command sets the interval, which the system waits to user input in http sessions before automatic logoff. To restore the default configuration, use the no form of this command.

Syntax

ip http exec-timeout *minutes* [*seconds*]

no ip http exec-timeout

Parameters

- *minutes* — Integer that specifies the number of minutes. (Range: 0-65535)
- *seconds* — Additional time intervals in seconds. (Range: 0-59)

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

User Guidelines

This command also configures the exec-timeout for HTTPS in case the HTTPS timeout was not set.

To specify no timeout, enter the ip https exec-timeout 0 0 command.

ip https server

The **ip https server** Global Configuration mode command enables configuring the device from a secured browser. To restore the default configuration, use the **no** form of this command.

Syntax

ip https server

no ip https server

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **crypto certificate generate** Global Configuration mode command to generate an HTTPS certificate.

Example

The following example enables configuring the device from a secured browser.

```
Console(config)# ip https server
```

ip https port

The **ip https port** Global Configuration mode command specifies the TCP port used by the server to configure the device through the Web browser. To restore the default configuration, use the **no** form of this command.

Syntax

i**p https port** *port-number*

no ip https port

Parameters

- *port-number* — Port number to be used by the HTTP server. (Range: 1-65535)

Default Configuration

The default port number is 443.

Command Mode

Global Configuration mode

User Guidelines

Specifying 0 as the port number effectively disables HTTP access to the device.

Example

The following example configures the https port number to 100.

Console(config)# ip https port 100

```
Console(config)# ip https port 100
```

crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed HTTPS certificate.

Syntax

crypto certificate [*number*] **generate** [**key-generate** *length*] [**cn** *common- name*] [**ou** *organization-unit]* [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)
- **key-generate** — Regenerate the SSL RSA key.
- *length* — Specifies the SSL RSA key length. (Range: 512-2048)

- *common- name* — Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- *organization* — Specifies the organization name. (Range: 1-64)
- *organization-unit* — Specifies the organization-unit or department name.(Range: 1-64)
- *location* — Specifies the location or city name. (Range: 1-64)
- *state* — Specifies the state or province name. (Range: 1-64)
- *country* — Specifies the country name. (Range: 2-2)
- *days* — Specifies number of days certification is valid. (Range: 30-3650)

Default Configuration

The Certificate and SSL's RSA key pairs do not exist.

If no RSA key length is specified, the default length is 1024.

If no URL or IP address is specified, the default common name is the lowest IP address of the device at the time that the certificate is generated.

If the number of days is not specified, the default period of time that the certification is valid is 365 days.

Command Mode

Global Configuration mode

User Guidelines

The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Use this command to generate a self-signed certificate for the device.

If the RSA keys do not exist, parameter **key-generate** must be used.

Example

The following example regenerates an HTTPS certificate.

```
Console(config)# crypto certificate 1 generate key-generate
```

crypto certificate request

The **crypto certificate request** Privileged EXEC mode command generates and displays certificate requests for HTTPS.

Syntax

crypto certificate *number* **request** [**cn** *common- name*][**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*]

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)
- *common- name* — Specifies the fully qualified URL or IP address of the device. (Range: 1- 64)
- *organization-unit* — Specifies the organization-unit or department name. (Range: 1-64)
- *organization* — Specifies the organization name. (Range: 1-64)
- *location* — Specifies the location or city name. (Range: 1-64)
- *state* — Specifies the state or province name. (Range: 1-64)
- *country* — Specifies the country name. (Range: 2-2)

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request you must first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command. Be aware that you have to reenter the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example

The following example generates and displays a certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa

g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
CN= router.gm.com
0= General Motors
C= US
```

crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by the Certification Authority for HTTPS.

Syntax

crypto certificate *number* **import**

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, enter an empty line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** Privileged EXEC mode command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Example

The following example imports a certificate signed by Certification Authority for HTTPS.

```
Console(config)# crypto certificate 1 import

-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

ip https certificate

The **ip https certificate** Global Configuration mode command configures the active certificate for HTTPS. To return to the default configuration, use the **no** form of this command.

Syntax

ip https certificate *number*

no ip https certificate

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

User Guidelines

The crypto certificate generate command should be used to generate HTTPS certificates.

Example

The following example configures the active certificate for HTTPS.

```
Console(config)# ip https certificate 1
```

show crypto certificate mycertificate

The **show crypto certificate mycertificate** Privileged EXEC mode command displays the SSH certificates of the device.

Syntax

show crypto certificate mycertificate [*number*]

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the certificate.

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
MIICFTCCAX4CAQAwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCICAxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxFDASBgNVBAMTCzEwLjYuNDEuMTM4MQowCAYDVQQK
EwEgMQowCAYDVQQLEwEgMB4XDTAzMDQzMDIwNTE1NFoXDTA0MDQyOTIwNTE1NFow
UzELMAkGA1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxFDASBgNVBAMT
CzEwLjYuNDEuMTM4MQowCAYDVQQKEwEgMQowCAYDVQQLEwEgMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQDrQxdrGjKwJMtq6YDF4aAoCnY2vXTivToJEn9vI55y
eIwn4n2dH1fKCxhnvJSmMk+jtA9pbQTALSWCm2S3jllZyWsE/tnnPUkkuNtApBa6
6OOy80lpYdpJuSJ8V/0wwvLYooh9h3PDDhSuWaWzCAlV94g1UzkNvrBsGEL5TPEp
BQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBADjg8wGBLdVHQVAOAo89zV2ZbpYbSxR9
RwJ4P6VaFRh2xnpDZXRASp482Tan9SQcUWcVIq2iFIKggXYeMSoHOB+0M+pf77PC
/m9UHVoHTjssPSAsU/7OGMGXVRFri0XhPgety9xsR+9zE1q2vPrrl7PW/+kupb3J
ZRZ/KAct/5zl
-----END CERTIFICATE-----
 Issued by : C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 Valid From: Apr 30 20:51:54 2003 GMT
 Valid to: Apr 29 20:51:54 2004 GMT
 Subject: C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 SHA1 Fingerprint: B3536E86 9487B229 C0A44199 DAB98046 7861F705
```

show ip http

The **show ip http** Privileged EXEC mode command displays the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip http
HTTP server enabled. Port: 80
```

show ip https

The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax

show ip https

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip https
HTTPS server enabled. Port: 443
Certificate 1 is not active.
 Issued by : C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 Valid From: Apr 30 20:51:54 2003 GMT
 Valid to: Apr 29 20:51:54 2004 GMT
 Subject: C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 SHA1 Fingerprint: B3536E86 9487B229 C0A44199 DAB98046 7861F705
Certificate 2 is active.
 Issued by : C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 Valid From: Apr 30 22:16:01 2003 GMT
 Valid to: Apr 29 22:16:01 2004 GMT
 Subject: C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 SHA1 Fingerprint: 3DBDF89B 6B3E46A2 4255D023 42A361F2 90ED7042
```

27 TACACS+ COMMANDS

tacacs-server host

The **tacacs-server host** Global Configuration mode command specifies a TACACS+ host. To delete the specified name or address, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]

no tacacs-server host {i*p-address* | *hostname*}

Parameters

- *ip-address* — IP address of the TACACS+ server.
- *hostname* — Host name of the TACACS+ server. (Range: 1-158 characters)
- **single-connection** — Indicates a single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the device and the daemon.
- *port-number* — Specifies a server port number. The host is not used for authentication if the port number is set to 0. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)
- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter " ". (Range: 0-128 characters)

- *source* — Specifies the source IP address to use for the communication. 0.0.0.0 indicates a request to use the IP address of the outgoing IP interface.
- *priority* — Determines the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified.

If no port number is specified, default port number 49 is used.

If no host-specific timeout, key-string or source value is specified, the global value is used.

If no TACACS+ server priority is specified, default priority 0 is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

Example

The following example specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```

tacacs-server key

The **tacacs-server key** Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key *key-string*

no tacacs-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+

server. This key must match the encryption used on the TACACS+ daemon. (Range: 0-128 characters)

Default Configuration

Empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the authentication encryption key for all TACACS+ servers.

```
Console(config)# tacacs-server key enterprise
```

tacacs-server timeout

The **tacacs-server timeout** Global Configuration mode command sets the interval during which the device waits for a TACACS+ server to reply. To restore the default configuration, use the **no** form of this command.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)

Default Configuration

5 seconds

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the timeout value to 30 for all TACACS+ servers.

```
Console(config)# tacacs-server timeout 30
```

tacacs-server source-ip

The **tacacs-server source-ip** Global Configuration mode command configures the source IP address to be used for communication with TACACS+ servers. To restore the default configuration, use the **no** form of this command.

Syntax

tacacs-server source-ip *source*

no tacacs-server source-ip *source*

Parameters

- *source* — Specifies the source IP address.

Default Configuration

The source IP address is the address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the source IP address for all TACACS+ servers.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

show tacacs

The **show tacacs** Privileged EXEC mode command displays configuration and statistical information about a TACACS+ server.

Syntax

show tacacs [*ip-address*]

Parameters

- *ip-address* — Name or IP address of the TACACS+ server.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays configuration and statistical information about a TACACS+ server.

```
Console# show tacacs


Device Configuration
--------------------


IP       Status   Port     Single   TimeOu   Source   Priority
addres                     Connec   t        IP
s                          tion
------   ------   ----     ------   ------   ------   --------
----                       ------   -        ---
                           -----
172.16   Connec   49       No       Global   Global   1
.1.1     ted
```

```
Global values

-------------

TimeOut: 3
```

28 SYSLOG COMMANDS

logging on

The **logging on** Global Configuration mode command controls error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the distribution of logging messages at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging** on command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example enables logging error messages.

```
Console(config)# logging on
```

logging

The **logging** Global Configuration mode command logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

logging {*ip-address* | *hostname*} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the host to be used as a syslog server.
- *hostname* — Specifies the host name of the syslog server. (Range: 1-158 characters)
- *port* — Specifies the port number for syslog messages. (Range: 1-65535)
- *level* — Specifies the severity level of logged messages sent to the syslog servers. Possible values: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging**.
- *facility* — Specifies the facility that is indicated in the message. Possible values: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**.
- *text* — Syslog server description. (Range: 1-64 characters)

Default Configuration

The default port number is 514.

The default logging message level is **informational**.

The default facility is local7.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 syslog servers can be used.

If no specific severity level is specified, the global values apply to each server.

Example

The following example limits logged messages sent to the syslog server with IP address 10.1.1.1 to severity level **critical**.

```
Console(config)# logging 10.1.1.1 severity critical
```

logging console

The **logging console** Global Configuration mode command limits messages logged to the console based on severity. To disable logging to the console, use the **no** form of this command.

Syntax

logging console *level*

no logging console

Parameters

- *level* — Specifies the severity level of logged messages displayed on the console. The possible values are: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

Default Configuration

The default severity level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits logging messages displayed on the console to severity level **errors**.

```
Console(config)# logging console errors
```

logging buffered

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. To cancel using the buffer, use the **no** form of this command.

Syntax

l**ogging buffered** *level*

no logging buffered

Parameters

- *level* — Specifies the severity level of messages logged in the buffer. The possible values are: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, **debugging**.

Default Configuration

The default severity level is informational.

Command Mode

Global Configuration mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on severity level **debugging**.

```
Console(config)# logging buffered debugging
```

logging buffered size

The **logging buffered size** Global Configuration mode command changes the number of syslog messages stored in the internal buffer. To restore the default configuration, use the **no** form of this command.

Syntax

logging buffered size *number*

no logging buffered size

Parameters

- *number* — Specifies the maximum number of messages stored in the history table. (Range: 20-400)

Default Configuration

The default number of messages is 200.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after Reset.

Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console(config)# logging buffered size 300
```

clear logging

The **clear logging** Privileged EXEC mode command clears messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the internal logging buffer.

```
Console# clear logging
Clear Logging File [y/n]
```

logging file

The **logging file** Global Configuration mode command limits syslog messages sent to the logging file based on severity. To cancel using the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

Parameters

- *level* — Specifies the severity level of syslog messages sent to the logging file. Possible values are: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging**.

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits syslog messages sent to the logging file based on severity level alerts.

```
Console(config)# logging file alerts
```

clear logging file

The **clear logging file** Privileged EXEC mode command clears messages from the logging file.

Syntax

clear logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]
```

aaa logging

The **aaa logging** Global Configuration mode command enables logging AAA login events. To disable logging AAA login events, use the **no** form of this command.

Syntax

aaa logging login

no aaa logging login

Parameters

- **login** — Indicates logging messages related to successful login events, unsuccessful login events and other login-related events.

Default Configuration

Logging AAA login events is enabled.

Command Mode

Global Configuration mode

User Guidelines

Other types of AAA events are not subject to this command.

Example

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

file-system logging

The **file-system logging** Global Configuration mode command enables logging file system events. To disable logging file system events, use the **no** form of this command.

Syntax

file-system logging copy

no file-system logging copy

file-system logging delete-rename

no file-system logging delete-rename

Parameters

- **copy** — Indicates logging messages related to file copy operations.
- **delete-rename** — Indicates logging messages related to file deletion and renaming operations.

Default Configuration

Logging file system events is enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

management logging

The **management logging** Global Configuration command enables logging management access list (ACL) events. To disable logging management access list events, use the **no** form of this command.

Syntax

management logging deny

no management logging deny

Parameters

- **deny** — Indicates logging messages related to deny actions of management ACLs.

Default Configuration

Logging management ACL events is enabled.

Command Mode

Global Configuration mode

User Guidelines

Other types of management ACL events are not subject to this command.

Example

The following example enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```

show logging

The **show logging** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
Console# show logging


Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200
Max.
File logging: level notifications. File Messages: 0 Dropped
(severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control
Application           Event                 Status
-----------           -----                 ------
AAA                   Login                 Enabled
File system           Copy                  Enabled
File system           Delete-Rename         Enabled
Management ACL        Deny                  Enabled


Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg0,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg1,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg2,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg3,
changed state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console
```

```
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet0, changed state to down

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet3, changed state to down
```

show logging file

The **show logging file** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the logging state and the syslog messages stored in the logging file.

```
Console# show logging file


Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200
Max.
File logging: level notifications. File Messages: 0 Dropped
(severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control
Application           Event                 Status
-----------           -----                 ------
AAA                   Login                 Enabled
File system           Copy                  Enabled
File system           Delete-Rename         Enabled
Management ACL        Deny                  Enabled


Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg0,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg1,
changed state to up
```

```
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg2,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernetg3,
changed state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet0, changed state to down

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet3, changed state to down
```

show syslog-servers

The **show syslog-servers** Privileged EXEC mode command displays the settings of the syslog servers.

Syntax

s**how syslog-servers**

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the settings of the syslog servers.

```
Console# show syslog-servers


Device Configuration
```

```
IP address    Port          Severity      Facility      Description

-----------   ----          -----------   --------      -----------
-                           --

192.180.2.2   514           Information   local7
7                           al

192.180.2.2   514           Warning       local7
8
```

29 WIRELESS AP BSS COMMANDS

bss

The **bss** Interface Radio Configuration mode command adds or removes ESS to/from a radio interface.

Syntax

bss {**add** {*ess-index* | *ssid*} | **remove** {*ess-index* | *ssid*}}

Parameters

- *ess-index* — The ESS index. (Range: 1-65535)
- *ssid* — The SSID string of the ESS. (Range: 1-32 characters)

Default Configuration

The default ESS is automatically added to the radio interface.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds an ESS to a radio interface called 'enterprise'.

```
Config# wlan ap CR1 config
Console (Config-ap)# interface radio 802.11g
Console (Config-ap-radio-if)# bss add enterprise
```

bss enable

The **bss enable** Interface Radio Configuration mode command places the device in BSS configuration mode.

Syntax

bss enable {*index* | *ssid*}

Parameters

- *index* — The ESS index. (Range: 1-65535)
- *ssid* — The SSID string of the ESS. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example places SSID device called ‘enterprise’ in BSS Configuration mode.

```
Console (Config-ap-radio-if)#c bss enable
Console (Config-ap-radio-if)# bss enable enterprise
Console (Config-ap-bss-if)#
```

advertise-ssid

The **advertise-ssid** BSS Configuration mode command advertises the BSS SSID. To disable advertising, use the **no** form of this command.

Syntax

advertise-ssid

no advertise-ssid

Parameters

This command has no keywords or arguments.

Default Configuration

The BSS SSID is advertised.

Command Mode

BSS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example advertises the BSS SSID.

```
Console (Config-ap-radio-if)# bss configure enterprise
Console (Config-ap-bss-if)#
```

data-rates

The **data-rates** BSS Configuration mode command configures the data rates used in a BSS. To restore defaults, use the **no f**orm of this command.

Syntax

data-rates {[**mandatory**] **add | remove**} rate1 [rate1…12]

no data-rates

The command can be implemented as follows:

data-rates mandatory add *rate1* [*rate1…12*]

data-rates {**add | remove}** *rate1* [*rate1…12*]

Parameters

- *rate-list* — Specifies the data rates that should be supported. Available rates are as follows:

  802.11g — 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54.

  802.11a — 6, 9, 12, 18, 24, 36, 48 and 54.

Default Configuration

All rates are optional except for the following rates that are mandatory:

- 802.11g: 1.
- 802.11a: 6.

Command Mode

BSS Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the data rates used in a BSS to 2 while complying with 802.11g.

```
Console (Config-ap-radio)# bss configure enterprise
Console (Config-wlan-ap-radio-bss-if)# data-rates mandatory add
2
```

30 SYSTEM MANAGEMENT COMMANDS

ping

The **ping** User EXEC mode command sends ICMP echo request packets to another node on the network.

Syntax

ping {*ip-address* | *hostname*}[**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

Parameters

- *ip-address* — IP address to ping.
- *hostname* — Host name to ping. (Range: 1-158 characters)
- *packet_size* — Number of bytes in a packet. The actual packet size is eight bytes larger than the specified size specified because the device adds header information. (Range: 56-1472 bytes)
- *packet_count* — Number of packets to send. If 0 is entered, it pings until stopped. (Range: 0-65535 packets)
- *time_out* — Timeout in milliseconds to wait for each reply. (Range: 50-65535 milliseconds)

Default Configuration

Default packet size is 56 bytes.

Default number of packets to send is 4.

Default timeout value is 2000 milliseconds.

Command Mode

User EXEC mode

User Guidelines

Press Esc to stop pinging.

Following are examples of unsuccessful pinging:

Destination does not respond. If the host does not respond, a “no answer from host” appears in ten seconds.

Destination unreachable. The gateway for this destination indicates that the destination is unreachable.

Network or host unreachable. The device found no corresponding entry in the route table.

Example

The following example displays pinging results:

```
Console> ping 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:


64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms


----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11


Console> ping yahoo.com
Pinging yahoo.com 66.218.71.198 with 64 bytes of data:


64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms


----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

traceroute

The **traceroute** User EXEC mode command discovers routes that packets actually take when traveling to their destination.

Syntax

traceroute {*ip-address* |*hostname*}[**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout time_out**] [**source** i*p-address*] [**tos** *tos*]

Parameters

- *ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)
- *packet_size* — Number of bytes in a packet. (Range: 40-1472)
- *max-ttl* — The largest TTL value that can be used. The traceroute command terminates when the destination is reached or when this value is reached. (Range:1-255)
- *packet_count* — The number of probes to be sent at each TTL level. (Range:1-10)
- *time_out* — The number of seconds to wait for a response to a probe packet.
- (Range:1-60)
- *ip-address* — One of the device's interface addresses to use as a source address for the probes. The device normally selects what it feels is the best source address to use.
- *tos* — The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Default Configuration

The default number of bytes in a packet is 40.

The default maximum TTL value is 30.

The default number of probes to be sent at each TTL level is 3.

The default timeout interval in seconds is 3.

Command Mode

User EXEC mode

User Guidelines

The **traceroute** command takesadvantage of the error messages generated by the devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate device has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace by pressing **Esc**.

Example

The following example discovers the routes that packets will actually take when traveling to their destination.

```
Console> traceroute umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu
(141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1
msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec
35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45 msec
45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54
msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57
msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58
msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec
63 msec
```

The following table describes significant fields shown above.

Field	Description
1	Indicates the sequence number of the device in the path to the host.
i2-gateway.stanford.edu	Host name of this device.
192.68.191.83	IP address of this device.
1 msec 1 msec 1 msec	Round-trip time for each probe sent.

The following table describes characters that may appear in the traceroute command output.

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation is required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded.
S	Source route failed.
U	Port unreachable.

telnet

The **telnet** User EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1*......]

Parameters

- *ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)
- *port* — A decimal TCP port number, or one of the keywords listed in the Ports table in the User Guidelines.
- *keyword* — One or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (decimal23) on the host.

Command Mode

User EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	**Purpose**
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, Telnet commands can be listed by pressing the Ctrl-shift-6-? keys at the system prompt.

A sample of this list follows. Note that the Ctrl-shift-6 sequence appears as ^^ on the screen.

```
Console> ‘Ctrl-shift-6’ ?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system command
prompt)
```

Several concurrent Telnet sessions can be opened and switched. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the **telnet** User EXEC mode command.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Return to System Command Prompt

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119

Keyword	Description	Port Number
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

This command lists concurrent telnet connections to remote hosts that were opened by the current telnet session to the local device. It does not list telnet connections to remote hosts that were opened by other telnet sessions.

Example

The following example displays connecting to 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

resume

The **resume** User EXEC mode command enables switching to another open Telnet session.

Syntax

resume [*connection*]

Parameters

- *connection* — The connection number. (Range: 1-4 connections)

Default Configuration

The default connection number is that of the most recent connection.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following command switches to open Telnet session number 1.

```
Console> resume 1
```

reload

The **reload** Privileged EXEC mode command reloads the operating system.

Syntax

reload

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

Example

The following example reloads the operating system.

```
Console# reload
This command will reset the whole system and disconnect your
current session. Do you want to continue (y/n) [n]?
```

hostname

The **hostname** Global Configuration mode command specifies or modifies the device host name. To remove the existing host name, use the **no** form of the command.

Syntax

hostname name

no hostname

Parameters

- *name* — The host name. of the device. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the device host name.

```
Console(config)# hostname enterprise
enterprise(config)#
```

show users

The **show users** Privileged EXEC mode command displays information about the active users.

Syntax

show users

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the active users.

```
Console# show users


Username              Protocol              Location
----------            -----------           ------------
Bob                   Serial
John                  SSH                   172.16.0.1
Robert                HTTP                  172.16.0.8
Betty                 Telnet                172.16.1.7
```

show sessions

The **show sessions** Privileged EXEC mode command lists open Telnet sessions.

Syntax

show sessions

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example lists open Telnet sessions.

```
Console# show sessions
```

```
Connection    Host          Address       Port          Byte
----------    -----------   ----------    -----         ----
              --
1             Remote        172.16.1.1    23            89
              device
2             172.16.1.2    172.16.1.2    23            8
```

The following table describes significant fields shown above.

Field	Description
Connection	Connection number.
Host	Remote host to which the device is connected through a Telnet session.
Address	IP address of the remote host.
Port	Telnet TCP port number
Byte	Number of unread bytes for the user to see on the connection.

show system

The **show system** Privileged EXEC mode command displays system information.

Syntax

show system

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the system information.

```
Console# show system
System Description:    Ethernet Switch
System Up Time        01,12:00:02
(days, hour:min:sec)

System Contact:       <contact name>

System Name:          <device name>

System Location:      <location>

System MAC Address:   00:11:22:33:44:55

System Object ID:     1.3.6.1.4.1.43.1.20.24


Unit                  Temperature (Celsius)    Status

-----------           -----------              -----------

1                     0                        UNAVAILABLE
```

show version

The **show version** Privileged EXEC mode command displays system version information.

Syntax

show version [**unit** unit]

Parameters

- *unit*— Specifies the number of the unit. (Range: 1-8)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays system version information (only for demonstration purposes).

```
Console# show version



Unit             SW version       Boot version     HW version
----             ----------       ------------     ----------
1                1.0.0.0          2.178            1.0.0
2                1.0.0.0          2.178            1.0.0
```

service cpu-utilization

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. To restore the default configuration, use the no form of this command.

Syntax

service cpu-utilization

no service cpu-utilization

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **show cpu utilization** Privileged EXEC command to view information on CPU utilization.

Example

This example enables measuring CPU utilization.

```
Console(config)# service cpu-utilization
```

show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax

show cpu utilization

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the service cpu-utilization Global Configuration mode command to enable measuring CPU utilization.

Example

The following example configures the CPU utilization information display.

```
Console# show cpu utilization

CPU utilization service is on.

CPU utilization
--------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

31 USER INTERFACE COMMANDS

enable

The **enable** Privileged EXEC mode command enters the Privileged EXEC mode.

Syntax

enable [*privilege-level*]

Parameters

- *privilege-level* — Privilege level to enter the system. (Range: 1-15)

Default Configuration

The default privilege level is 15.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode:

```
Console> enable
enter password:
Console#
```

disable

The **disable** Privileged EXEC mode command returns to the User EXEC mode.

Syntax

disable [*privilege-level]*

Parameters

- *privilege-level* — Privilege level to enter the system. (Range: 1-15)

Default Configuration

The default privilege level is 1.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example return to Users EXEC mode.

```
Console# disable
Console>
```

login

The **login** User EXEC mode command changes a login username.

Syntax

login

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode and logs in with username **admin**.

```
Console> login
User Name:admin
Password:*****
Console#
```

configure

The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax

configure

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Global Configuration mode.

```
Console# configure
Console(config)#
```

exit (Configuration)

The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
Console(config-if)# exit
Console(config)# exit
Console#
```

exit

The **exit** Privileged/User EXEC mode command closes an active terminal session by logging off the device.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
Console> ex1.7it
```

end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax

end

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes.

User Guidelines

There are no user guidelines for this command.

Example

The following example changes from Global Configuration mode to Privileged EXEC mode.

```
Console(config)# end
Console#
```

help

The **help** command displays a brief description of the help system.

Syntax

help

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Example

The following example describes the help system.

```
Console# help

Help may be requested at any point in a command by entering a
question mark '?'. If nothing matches the currently entered
incomplete command, the help list is empty. This indicates that
for a query at this point, there is no command matching the
current input. If the request is within a command, enter backspace
and erase the entered characters to a point where the request
results in a display.
Help is provided when:
1. There is a valid command and a help request is made for
entering a parameter or argument (e.g. 'show ?'). All possible
parameters or arguments for the entered command are displayed.
2. An abbreviated argument is entered and a help request is made
for arguments matching the input (e.g. 'show pr?').
```

terminal data-dump

The **terminal data-dump** User EXEC mode command enables dumping all the output of a show command without prompting. To disable dumping, use the **no** form of this command.

Syntax

terminal data-dump

no terminal data-dump

Default Configuration

Dumping is disabled.

Command Mode

User EXEC mode

User Guidelines

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the Spacebar displays the next screen of output. The data-dump command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

Example

This example dumps all output immediately after entering a show command.

```
Console> terminal data-dump
```

debug-mode

The **debug-mode** Privileged EXEC Command mode switches to debug mode.

Syntax

debug-mode

Default Configuration

This command has no default configuration.

Command Mode

Privilaged EXEC

User Guidelines

There are no user guidelines for this command.

show history

The **show history** Privileged EXEC mode command lists the commands entered in the current session.

Syntax

show history

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show version

SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0


Console# show clock

15:29:03 Jun 17 2005
```

```
Console# show history

show version
show clock
show history
3 commands were logged (buffer size is 10)
```

show privilege

The **show privilege** Privileged/User EXEC mode command displays the current privilege level.

Syntax

show privilege

Default Configuration

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the current privilege level for the Privileged EXEC mode.

```
Console# show privilege
Current privilege level is 15
```

32 GVRP Commands

gvrp enable (Global)

GARP VLAN Registration Protocol (GVRP) is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single device is manually configured with all desired VLANs for the network, and all other devices on the network learn these VLANs dynamically.

The **gvrp enable** Global Configuration mode command enables GVRP globally. To disable GVRP on the device, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

gvrp enable (Interface)

The **gvrp enable** Interface Configuration (Ethernet, port-channel) mode command enables GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member in only one VLAN.

Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID is manually defined as the untagged VLAN VID.

Example

The following example enables GVRP on Ethernet port g6.

```
Console(config)# interface ethernet g6
Console(config-if)# gvrp enable
```

garp timer

The **garp timer** Interface Configuration (Ethernet, Port channel) mode command adjusts the values of the join, leave and leaveall timers of GARP applications. To restore the default configuration, use the **no** form of this command.

Syntax

garp timer {join | leave | leaveall} *timer_value*

no garp timer

Parameters

- {**join** | **leave** | **leaveall**} — Indicates the type of timer.
- *timer_value* — Timer values in milliseconds in multiples of 10. (Range: 10-2147483640)

Default Configuration

Following are the default timer values:

- Join timer — 200 milliseconds
- Leave timer — 600 milliseconds
- Leavall timer — 10000 milliseconds

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The following relationship must be maintained between the timers:

Leave time must be greater than or equal to three times the join time.

Leave-all time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

Example

The following example sets the leave timer for Ethernet port g6 to 900 milliseconds.

```
Console(config)# interface ethernet g6
Console(config-if)# garp timer leave 900
```

gvrp vlan-creation-forbid

The **gvrp vlan-creation-forbid** Interface Configuration (Ethernet, port-channel) mode command disables dynamic VLAN creation or modification. To enable dynamic VLAN creation or modification, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

Dynamic VLAN creation or modification is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

Example

The following example disables dynamic VLAN creation on Ethernet port 1.

```
Console(config)# interface eth7ernet 1
Console(config-if)# gvrp vlan-creation-forbid
```

gvrp registration-forbid

The **gvrp registration-forbid** Interface Configuration (Ethernet, port-channel) mode command deregisters all dynamic VLANs on a port and prevents VLAN creation or registration on the port. To allow dynamic registration of VLANs on a port, use the **no f**orm of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forbids dynamic registration of VLANs on Ethernet port g1.

```
Console(config)# interface ethernet g1
Console(config-if)# gvrp registration-forbid
```

clear gvrp statistics

The **clear gvrp statistics** Privileged EXEC mode command clears all GVRP statistical information.

Syntax

clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: unit/port)
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears all GVRP statistical information on Ethernet port g1.

```
Console# clear gvrp statistics ethernet g1
```

show gvrp configuration

The **show gvrp configuration** Privieged EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax

show gvrp configuration [**ethernet** *interface* | **port-channel** *port-channel-number]*

Parameters

- *interface* — A valid Ethernet port. Elana
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privieged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP configuration information.

```
Console# show gvrp configuration


GVRP Feature is currently enabled on the device.


                                       Timers (milliseconds)
```

```
Port(s)  Status   Registr  Dynamic  Join     Leave    Leave
                  ation    VLAN                       All
                           Creatio
                           n

------   -------  -------  -------  ----     -----    -------
                  -----    ----                       --

g1       Enabled  Normal   Enabled  200      600      10000

g4       Enabled  Normal   Enabled  200      600      10000
```

show gvrp statistics

The **show gvrp statistics** Privieged EXEC mode command displays GVRP statistics.

Syntax

show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. Elana
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privieged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows GVRP statistical information.

```
Console# show gvrp configuration


GVRP Feature is currently enabled on the device.

```

```
                                Timers (milliseconds)

Port(   Statu   Regis   Dynam   Join    Leave   Leave All
s)      s       trati   ic
                on      VLAN
                        Creat
                        ion

-----   -----   -----   -----   ----    -----   ---------
-       --      -----   -----
                --      -

g1      Enabl   Norma   Enabl   200     600     10000
        ed      l       ed

g4      Enabl   Norma   Enabl   200     600     10000
        ed      l       ed
```

show gvrp error-statistics

The **show gvrp error-statistics** Privieged EXEC mode command displays GVRP error statistics.

Syntax

show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. Elana
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privieged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP statistical information.

```
Console# show gvrp error-statistics

GVRP Error Statistics:

Legend:

INVPROT :    Invalid                 INVALEN :    Invalid
             Protocol Id                          Attribute
                                                  Length

INVATYP :    Invalid                 INVEVENT:    Invalid
             Attribute                            Event
             Type

INVAVAL :    Invalid
             Attribute
             Value

 Port INVPROT INVATYP INVAVAL INVALEN INVEVENT
```

33 VLAN COMMANDS

vlan database

The **vlan database** Global Configuration mode command enters the VLAN Configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-vlan)#
```

vlan

Use the **vlan** VLAN Database mode command to create a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan *vlan-range*

no vlan vlan-range

Parameters

- vlan-range — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs. (Range: 2-4094)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

The following example VLAN number 1972 is created.

```
Console(config)# vlan database
Console(config-vlan)# vlan 1972
```

interface vlan

The **interface vlan** Global Configuration mode command enters the Interface Configuration (VLAN) mode.

Syntax

i**nterface vlan** *vlan-id*

Parameters

- *vlan-id* — Specifies an existing VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures VLAN 1 with IP address 131.108.1.27.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27
```

interface range vlan

The **interface range vlan** Global Configuration mode command enables simultaneously configuring multiple VLANs.

Syntax

interface range vlan {*vlan-range* | **all**}

Parameters

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs. (Range: 2-4094)
- **all** — All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution of the command continues on the other interfaces.

Configuring all ports may consume an excessive amount of time. Define only the required ports to save time.

Example

The following example groups VLANs 221, 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228,889
Console(config-if)#
```

name

The **name** Interface Configuration mode command adds a name to a VLAN. To remove the VLAN name, use the no form of this command.

Syntax

name string

no name

Parameters

- *string* — Unique name to be associated with this VLAN.

  (Range: 1-32 characters)

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. Cannot be configured for a range of interfaces (range context).

User Guidelines

The name string may include numbers and other characters (#,@,% etc.) but no spaces.

Example

The following example gives VLAN number 19 the name **Marketing**.

```
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```

switchport access vlan

The **switchport access vlan** Interface Configuration mode command configures the VLAN ID when the interface is in access mode. To restore the default configuration, use the **no** form of this command.

Syntax

s**witchport access vlan** {*vlan-id* }

no switchport access vlan

Parameters

- *vlan-id* — Specifies the ID of the VLAN to which the port is configured.

Default Configuration

All ports belong to VLAN 1.

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode access
```

switchport trunk allowed vlan

The **switchport trunk** allowed vlan Interface Configuration mode command adds or removes VLANs to or from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — List of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — List of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds VLANs 1, 2, 5 to 6 to the allowed list of the 1

Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 1-2,5-6
```

switchport trunk native vlan

The **switchport trunk native vlan** Interface Configuration mode command defines the native VLAN when the interface is in trunk mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Parameters

- *vlan-id*— Specifies the ID of the native VLAN.

Default Configuration

VID=1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command adds the port as a member in native VLAN. If the port is already in the VLAN (as allowed) it will automatically change the last entry to native.

The command adds the port as a member in native VLAN 2. If the port is already configured as a native VLAN 3 it will automatically change the last entry (VLAN 2). Only one native VLAN can be configured to the port.

Example

The following example configures VLAN number 123 as the native VLAN when Ethernet port 1 is in trunk mode.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode trunk
Console(config-if)# switchport trunk native vlan 123
```

switchport general allowed vlan

The **switchport general allowed vlan** Interface Configuration mode command adds or removes VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-lis*t

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged** — Indicates that the port transmits tagged packets for the VLANs.
- **untagged** — Indicates that the port transmits untagged packets for the VLANs.

Default Configuration

If the port is added to a VLAN without specifying tagged or untagged, the default setting is tagged.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command enables changing the egress rule (for example from tagged to untagged) without first removing the VLAN from the list.

Example

The following example adds VLANs 2, 5, and 6 to the allowed list of Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general allowed vlan add 2,5-6
tagged
```

switchport general pvid

The **switchport general pvid** Interface Configuration mode command configures the PVID when the interface is in general mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

Parameters

- *vlan-id* — Specifies the PVID (Port VLAN ID).

Default Configuration

If the default VLAN is enabled, PVID = 1. Otherwise, PVID=4095.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the PVID for Ethernet port 1, when the interface is in general mode.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general pvid 234
```

switchport general ingress-filtering disable

The **switchport general ingress-filtering disable** Interface Configuration mode command disables port ingress filtering. To restore the default configuration, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables port ingress filtering on Ethernet port 1

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general ingress-filtering disable
```

switchport general acceptable-frame-type tagged-only

The **switchport general acceptable-frame-type tagged-only** Interface Configuration mode command discards untagged frames at ingress. To restore the default configuration, use the **no** form of this command.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port 1 to discard untagged frames at ingress.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general acceptable-frame-type
tagged-only
```

switchport forbidden vlan

The **switchport forbidden vlan** Interface Configuration mode command forbids adding specific VLANs to a port. To **restore** the default configuration, use the remove parameter for this command.

Syntax

switchport forbidden vlan {**add** *vlan-lis*t | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command can be used to prevent GVRP from automatically making the specified VLANs active on the selected ports.

Example

The following example forbids adding VLAN IDs 234 to 256 to Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode trunk
Console(config-if)# switchport forbidden vlan add 234-256
```

show vlan

The **show vlan** Privileged EXEC mode command displays VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

Parameters

- *vlan-id* — specifies a VLAN ID
- vlan-name — Specifies a VLAN name string. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan


VLAN          Name          Ports         Type          Authorizati
                                                        on

----          -------       --------      ----          -----------
                                                        --

1             default       1,2           other         Required

10            VLAN0010      1             dynamic       Required

11            VLAN0011      1             static        Required

20            VLAN0020      1             static        Required

21            VLAN0021                    static        Required

30            VLAN0030                    static        Required

31            VLAN0031                    static        Required

91            VLAN0011      1             static        Not
                                                        Required

3978          Guest VLAN    1             guest         -
```

show vlan internal usage

The **show vlan internal usage** Privileged EXEC mode command displays a list of VLANs used internally by the device.

Syntax

show vlan internal usage

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays VLANs used internally by the device.

```
Console# show vlan internal usage


Usage     VLAN            Reserved         IP address
--------  ----            --------         ----------
14        50              Yes              Inactive
```

show interfaces switchport

The **show interfaces switchport** Privileged EXEC mode command displays the switchport configuration.

Syntax

show interfaces switchport {**ethernet** *interface* | **port-channel** port-channel-number}

Parameters

- interface — A valid Ethernet port number.
- port-channel-number — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the switchport configuration for Ethernet port.

```
Console# show interfaces switchport ethernet g5
Port: g5
Port Mode: General
Gvrp Status: enabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN < NATIVE >: 1


Port is member in:


Vlan          Name             Engree rule     Membership Type
-------       -------          -------         -------
1             1                Untagged        System


Forbidden VLANS:
Vlan          Name
-------       -------


Classification rules:
Mac based VLANs
Group ID      Vlan ID
-------       -------


Subnet based VLANs:
Group ID      Vlan ID
-------       -------
```

34 802.1X COMMANDS

aaa authentication dot1x

The **aaa authentication dot1x** Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. To restore the default configuration, use the **no** form of this command.

Syntax

aaa authentication dot1x default *method1 [method2...]*

no aaa authentication dot1x default

Parameters

- *method1 [method2...]* — Specify at least one method from the following list:

Keyword	Description
RADIUS	Uses the list of all RADIUS servers for authentication
None	Uses no authentication

Default Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. To ensure that authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

The RADIUS server must support MD-5 challenge and EAP type frames.

Example

The following example uses the aaa authentication dot1x default command with no authentication.

```
Console# configure
Console(config)# aaa authentication dot1x default none
```

dot1x system-auth-control

The **dot1x system-auth-control** Global Configuration mode command enables 802.1x globally. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

802.1x is disabled globally.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

dot1x port-control

The **dot1x port-control** Interface Configuration mode command enables manually controlling the authorization state of the port. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Parameters

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the port and the client.
- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based authentication of the client.
- **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

Port is in the force-authorized state

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in auto state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

Example

The following example enables 802.1x authentication on Ethernet port 16.

```
Console(config)# interface ethernet 16
Console(config-if)# dot1x port-control auto
```

dot1x re-authentication

The **dot1x re-authentication** Interface Configuration mode command enables periodic re-authentication of the client. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables periodic re-authentication of the client.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x re-authentication
```

dot1x timeout re-authperiod

The **dot1x timeout re-authperiod** Interface Configuration mode command sets the number of seconds between re-authentication attempts. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameters

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300-4294967295)

Default Configuration

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the number of seconds between re-authentication attempts, to 300.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout re-authperiod 300
```

dot1x re-authenticate

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

Syntax

dot1x re-authenticate [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: unit/port)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following command manually initiates a re-authentication of 802.1x-enabled Ethernet port g16.

```
Console# dot1x re-authenticate ethernet g16
```

dot1x timeout quiet-period

The **dot1x timeout quiet-period** Interface Configuration mode command sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

- *seconds* — Specifies the time in seconds that the device remains in the quiet state following a failed authentication exchange with the client. (Range: 0-65535 seconds)

Default Configuration

Quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, a smaller number than the default value should be entered.

Example

The following example sets the number of seconds that the device remains in the quiet state following a failed authentication exchange to 3600.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout quiet-period 3600
```

dot1x timeout tx-period

The **dot1x timeout tx-period** Interface Configuration mode command sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

- *seconds* — Specifies the time in seconds that the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 1-65535 seconds)

Default Configuration

Timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers

Example

The following command sets the number of seconds that the device waits for a response to an EAP-request/identity frame, to 3600 seconds.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout tx-period 3600
```

dot1x max-req

The **dot1x max-req** Interface Configuration mode command sets the maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- *count* — Number of times that the device sends an EAP-request/identity frame before restarting the authentication process. (Range: 1-10)

Default Configuration

The default number of times is 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers

Example

The following example sets the number of times that the device sends an EAP-request/identity frame to 6.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x max-req 6
```

dot1x timeout supp-timeout

The **dot1x timeout supp-timeout** Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response to an EAP-request frame from the client before resending the request. (Range: 1-65535 seconds)

Default Configuration

Default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers

Example

The following example sets the timeout period before retransmitting an EAP-request frame to the client to 3600 seconds.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout server-timeout

The **dot1x timeout server-timeout** Interface Configuration mode command sets the time that the device waits for a response from the authentication server. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response from the authentication server.

  (Range: 1-65535 seconds)

Default Configuration

The timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout can be determined by comparing the **dot1x timeout server-timeout** value and the result of multiplying the **radius-server retransmit** value with the **radius-server timeout** value and selecting the lower of the two values.

Example

The following example sets the time for the retransmission of packets to the authentication server to 3600 seconds.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout server-timeout 3600
```

show dot1x

The **show dot1x** Privileged EXEC mode command displays the 802.1x status of the device or specified interface.

Syntax

show dot1x [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: unit/port)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status of 802.1x-enabled Ethernet ports.

```
Console# show dot1x


802.1x is enabled


Port      Admin     Oper      Reauth    Reauth    Username
          Mode      Mode      Control   Period

----      --------  --------  -------   ------    --------
          --        -

g1        Auto      Authoriz  Ena       3600      Bob
                    ed

g2        Auto      Authoriz  Ena       3600      John
                    ed

g3        Auto      Unauthor  Ena       3600      Clark
                    ized

g4        Force-au  Authoriz  Dis       3600      n/a
          th        ed

g5        Force-au  Unauthor  Dis       3600      n/a
          th        ized*


* Port is down or not present.


Console# show dot1x ethernet 3


802.1x is enabled.


Port      Admin     Oper      Reauth    Reauth    Username
          Mode      Mode      Control   Period

----      --------  --------  -------   ------    --------
          --        -

g3        Auto      Unauthor  Ena       3600      Clark
                    ized
```

```
Quiet period: 60 Seconds
Tx period:30 Seconds
Max req: 2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff

Authenticator State Machine
State: HELD

Backend State Machine
State: IDLE
Authentication success: 9
Authentication fails: 1
```

fThe following table describes the significant fields shown in the display.

Field	**Description**
Port	The port number.
Admin mode	The port admin mode. Possible values: Force-auth, Force-unauth, Auto.
Oper mode	The port oper mode. Possible values: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	The username representing the identity of the Supplicant. This field shows the username in case the port control is auto. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.

Field	Description
Quiet period	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Max req	The maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	Time in seconds the switch waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	Time in seconds the switch waits for a response from the authentication server before resending the request.
Session Time	The amount of time the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.
Termination Cause	The reason for the session termination.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	The number of times the state machine received a Success message from the Authentication Server.
Authentication fails	The number of times the state machine received a Failure message from the Authentication Server.

show dot1x users

The **show dot1x users** Privileged EXEC mode command displays active 802.1x authenticated users for the device.

Syntax

show dot1x users [**username** *username*]

Parameters

- *username* — Supplicant username (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x users.

```
Console# show dot1x users


Port          Username      Session       Auth Method    MAC
                            Time                        Address

-----         --------      -----------   -----------   -----------
                            -                           ---

g1            Bob           1d:03:08.58   Remote        0008:3b79:8
                                                        787

g2            John          08:19:17      None          0008:3b89:3
                                                        127


Console# show dot1x users username Bob


Username: Bob

Port          Username      Session       Auth Method    MAC
                            Time                        Address

-----         --------      -----------   -----------   -----------
                            -                           ---

g1            Bob           1d:03:08.58   Remote        0008:3b79:8
                                                        787
```

The following table describes the significant fields shown in the display.

Field	Description
Port	The port number.
Username	The username representing the identity of the Supplicant.
Session Time	The period of time the Supplicant is connected to the system.
Authentication Method	Authentication method used by the Supplicant to open the session.
MAC Address	MAC address of the Supplicant.

show dot1x statistics

The **show dot1x statistics** Privileged EXEC mode command displays 802.1x statistics for the specified interface.

Syntax

show dot1x statistics ethernet *interface*

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x statistics for the specified interface.

```
Console# show dot1x statistics ethernet 1


EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 12

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display.

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.

Field	Description
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

dot1x auth-not-req

The **dot1x auth-not-req** Interface Configuration (VLAN) mode command enables unauthorized devices access to the VLAN. To disable access to the VLAN, use the **no** form of this command.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

Access is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets would be accepted in the unauthorized state.)

Example

The following example enables access to the VLAN to unauthorized devices.

```
Console(config)# interface vlan 5
Console(config-if)# dot1x auth-not-req
```

dot1x multiple-hosts

The **dot1x multiple-hosts** Interface Configuration mode command enables multiple hosts (clients) on an 802.1x-authorized port, where the authorization state of the port is set to **auto**. To restore the default configuration, use the no form of this command.

Syntax

dot1x multiple-hosts

no dot1x multiple-hosts

Default Configuration

Multiple hosts are disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables the attachment of multiple clients to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

For unauthenticated VLANs, multiple hosts are always enabled.

Multiple-hosts must be enabled to enable port security on the port.

Example

The following command enables multiple hosts (clients) on an 802.1x-authorized port.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x multiple-hosts
```

dot1x single-host-violation

The **dot1x single-host-violation** Interface Configuration mode command configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the no form of this command to restore defaults.

Syntax

dot1x single-host-violation {**forward** | **discard** | **discard-shutdown**} [trap *seconds*]

no port dot1x single-host-violation

Parameters

- **forward** — Forwards frames with source addresses that are not the supplicant address, but does not learn the source addresses.
- **discard** — Discards frames with source addresses that are not the supplicant address.
- **discard-shutdown** — Discards frames with source addresses that are not the supplicant address. The port is also shut down.
- **trap** — Indicates that SNMP traps are sent.
- **seconds** — Specifies the minimum amount of time in seconds between consecutive traps.

  (Range: 1- 1000000)

Default Configuration

Frames with source addresses that are not the supplicant address are discarded.

No traps are sent.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command is relevant when multiple hosts is disabled and the user has been successfully authenticated.

Example

The following example forwards frames with source addresses that are not the supplicant address and sends consecutive traps at intervals of 100 seconds.

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x single-host-violation forward trap
100
```

dot1x guest-vlan

The **dot1x guest-vlan** Interface Configuration (VLAN) mode command defines a guest VLAN. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
Console#
Console# configure
Console(config)# vlan database
Console(config-vlan)# vlan 2
Console(config-vlan)# exit
Console(config)# interface vlan 2
Console(config-if)# dot1x guest-vlan
```

dot1x guest-vlan enable

The **dot1x vlans guest-vlan enable** Interface Configuration mode command enables unauthorized users on the interface access to the Guest VLAN. To disable access, use the **no** form of this command

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration

Disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

Example

The following example enables unauthorized users on Ethernet port 1 to access the guest VLAN.

```
Console# configure
Console(config)# interface ethernet g1
Console(config-if)# dot1x guest-vlan enable
```

show dot1x advanced

The **show dot1x advanced** Privileged EXEC mode command displays 802.1x advanced features for the device or specified interface.

Syntax

show dot1x advanced [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: unit/port)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x advanced features for the device.

```
Console# show dot1x advanced


Guest VLAN: 2

Unauthenticated VLANs: 91,92


Interface              Multiple Hosts         Guest VLAN

---------              --------------         ----------

g1                     Disabled               Enabled

g2                     Enabled                Disabled


Console# show dot1x advanced ethernet 1

Guest VLAN: 2

Unauthenticated VLANs: 91,92
```

```
Interface             Multiple Hosts         Guest VLAN
---------             --------------         ----------
g1                    Disabled               Enabled

Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```

35 WIRELESS AP RADIO COMMANDS

interface radio

The **interface radio** AP Configuration mode command places the device in Radio Configuration mode.

Syntax

interface radio {**802.11a** | **802.11g**}

Parameters

- **802.11a** — In accordance with 802.11a protocol.
- **802.11g** — In accordance with 802.11g protocol.

Default Configuration

This command has no default configuration.

Command Mode

AP Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example places the device in the Radio Configuration mode, complying with the 802.11a protocol.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-ap-radio-if)#
```

enable (ap radio)

The **enable** AP Interface Radio Configuration mode command administratively enables the radio. To administratively disable the radio, use the **no** form of this command.

Syntax

enable

no enable

Parameters

This command has no keywords or arguments.

Default Configuration

Enable.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

Use the **wlan tx-power off** Global Configuration command to globally enable/disable TX power. TX power is enabled on specific AP only if TX power is enabled globally and for the AP.

Example

The following example administratively enables the radio.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# enable
```

channel

The **channel** AP Interface Radio Configuration mode command configure the RF channel. To restore the default configuration, use the **no** form of this command.

Syntax

channel {*number* | *frequency* | **least-congested**}

no channel

Parameters

- *number* — Specifies a channel number. The ranges are as follows:
  - 802.11g — 1 – 14.
  - 802.11a — 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 149, 153, 157, 161.
- *frequency* — Specifies the center frequency for the radio channel. The ranges are as follows:
  - 802.11g — 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472, 2484.
  - 802.11a — 5170, 5180, 5190, 5200, 5210, 5220, 5230, 5240, 5260, 5280, 5300, 5320, 5745, 5765, 5785, 5805.
- **least-congested** — Enables or disables the scanning for a least busy radio channel.

Default Configuration

Least congested channel.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

The valid frequencies depend on the country code that was set by the **wlan country-code** Global Configuration command.

Example

The following example configures the RF channel to a 802.11g frequency of 2437

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# channel 802.11g 2437
```

power

The **power** AP Interface Radio Configuration mode command configures the power level. To restore the default configuration, use the **no** form of this command.

Syntax

power {**max** | **half** | **quarter** | **eighth** | **min**}

no power

Parameters

- **max** — Maximum power.
- **half** — Half of the maximum power.
- quarter — Quarter of the maximum power.
- **eighth** — Eighth of the maximum power.
- **min** — Minimum power.

Default Configuration

Maximum power.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

- The maximum power depends on the country code that was set by the **wlan country-cod**e Global Configuration command.
- The power is off if the **wlan tx-power off** Global Configuration command was activated.

Example

The following example configures the power level to half the maximum power.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# power half
```

allow traffic

The **allow traffic** AP Interface Radio Configuration mode command allows users traffic. To disallow users traffic, use the no form of this command.

Syntax

allow traffic

no allow traffic

Parameters

This command has no keywords or arguments.

Default Configuration

Users traffic is allowed.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example allows user traffic.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# allow traffic
```

preamble

The **preamble** AP Interface Radio Configuration mode command configures the preamble support for 802.11g transceivers. To restore default, use the **no** form of this command.

Syntax

preamble {long | short}

no preamble

Parameters

- **long** — The AP supports long and short preambles.
- **short** — The AP supports short preambles.

Command Mode

AP Interface Radio configuration mode

User Guidelines

This command is only relevant for 802.11g transceivers.

Example

The following example configures the preamble support for 802.11g transceivers to long.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# preamble long
```

rts threshold

The **rts threshold** AP Interface Radio Configuration mode command configures the Request-To-Send (RTS) threshold. To restore defaults, use the **no** form of this command.

Syntax

rts threshold *number*

no rts threshold

Parameters

- *number* — Specifies the packet size, in bytes, above which the access point negotiates an RTS/CTS before sending out the packet. (Range: 0-2347)

Default Configuration

The default RTS threshold is 2312 bytes.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the RTS threshold to 2300 bytes.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# rts threshold 2300
```

antenna

The **antenna** AP Interface Radio Configuration mode command configures an antenna for the transceiver. To restore defaults, use the **no** form of this command.

Syntax

antenna {**diversity** | **1** | **2**}

no antenna

Parameters

- **diversity** — Specifies the antenna with the best signal.
- **1** — Specifies antenna number 1.
- **2** — Specifies antenna number 2.

Default Configuration

Diversity

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures antenna 1 for the transceiver.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# antenna 1
```

beacon period

The **beacon period** AP Interface Radio Configuration mode command configures the beacon period. To restore defaults, use the **no** form of this command.

Syntax

beacon period *milliseconds*

no beacon period

Parameters

- *milliseconds* — Specifies the beacon time in milliseconds. (Range: 50 - 300)

Default Configuration

The default beacon period is 100 milliseconds.

Command Mode

AP Interface Radio Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the beacon period to 300 milliseconds.

```
Console (Config-wlan-ap)# interface radio 802.11g
Console (Config-wlan-ap-radio)# beacon period 300
```

36 Wireless WLAN Commands

wlan tx-power off

The **wlan tx-power off** Global Configuration mode command turns off all APs transmitters. To enable transmit Power, use the no form of this command.

Syntax

wlan tx-power off

no wlan tx-power off

Parameters

This command has no keywords or arguments.

Default Configuration

Auto

Command Mode

Global Configuration mode

User Guidelines

Use the enable **AP interface radio configuration** command to enable/disable TX power of specific AP.

TX power is enabled on a specific AP only if TX power is enabled globally and for the AP.

Example

The following example turns off all AP transmitters.

```
Console (config)# wlan tx-power off
```

wlan country-code

The **wlan country-code** Global Configuration mode command configures the country code in which the device is located and the physical location of AP connected to the device. To restore defaults, use the **no** form of this command.

Syntax

wlan country-code *code*

no wlan country-code

Parameters

- *code* — Specify the ISO country-code. See the user guidelines for a list of country codes.

Default Configuration

Product specific.

Command Mode

Global Configuration mode

User Guidelines

The following table lists the supported country codes.

Country	Code	Country	Code	Country	Code
Albania	AL	Greenland	GL	Pakistan	PK
Algeria	DZ	Gaudeloupe	GP	Panama	PA
Andorra	AD	Guatemala	GT	Paraguay	PY
Argentina	AR	Guyana	GY	Peru	PE
Armenia	AM	Holy See (Vatican City)	VA	Philippines	PH
Australia	AU	Hong Kong	HK	Poland	PL
Austria	AT	Hungary	HU	Portugal	PT
Azerbaijan	AZ	Iceland	IS	Puerto Rico	PR
Bahamas	BS	India	IN	Qatar	QA
Bahrain	BH	Indonesia	ID	Romania	RO

Country	**Code**	**Country**	**Code**	**Country**	**Code**
Belarus	BY	Iran	IR	Russian Federation	RU
Belgium	BE	Ireland	IE	San Marino	SM
Belize	BZ	Israel	IL	Saudi Arabia	SA
Bolivia	BO	Italy	IT	Serbia and Montenegro	CS
Bosnia and Herzogovina	BA	Japan	JP	Singapore	SG
Brazil	BR	Jordan	JO	Slovakia	SK
Brunei Darussalam	BN	Kazakhstan	KZ	Slovenia	SI
Bulgaria	BG	North Korea	KP	South Africa	ZA
Canada	CA	South Korea	KR	Spain	ES
Chile	CL	Kuwait	KW	Sri Lanka	LK
China	CN	Latvia	LV	Sweden	SE
Colombia	CO	Lebanon	LB	Switzerland	CH
Costa Rica	CR	Liechtenstein	LI	Syria	SY
Croatia	HR	Lithuania	LT	Taiwan, Province of China	TW
Cyprus	CY	Luxembourg	LU	Thailand	TH
Czech Republic	CZ	Macau	MO	Turkey	TR
Denmark	DK	Macedonia	MK	Ukraine	UA
Dominican Republic	DO	Malaysia	MY	United Arab Emirates	AE
Ecuador	EC	Martinique	MQ	United Kingdom	GB

Country	Code	Country	Code	Country	Code
Egypt	EG	Mexico	MX	United States	US
Estonia	EE	Moldova, Republic of	MD	Uruguay	UY
Finland	FI	Monaco	MC	Uzbekistan	UZ
France	FR	Morocco	MA	Venezuela	VE
Georgia	GE	Netherlands	NL	Vietnam	VN
Germany	DE	New Zealand	NZ	Virgin Islands (U.S.)	VI
Gibralter	GI	Norway	NO		
Greece	GR	Oman	OM		

Example

The following example configures the country code in which the device is located, as the US.

```
Console (config)# wlan country-code us
```

wlan tx-power auto enable

The **wlan tx-power auto enable** Global Configuration mode command enables Auto Transmit Power. To disable Auto Transmit Power, use the no form of this command.

Syntax

wlan tx-power auto enable

no wlan tx-power auto enable

Parameters

This command has no keywords or arguments.

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

The Auto Transmit Power algorithm adjusts the transmit power of APs, so the signal strength heard at the second-closest access point is as close as possible to the target signal-strength configured by the **wlan tx-power auto signal-strengt**h Global Configuration command.

Example

The following example enables Auto Transmit Power.

```
Console (config)# wlan tx-power auto enable
```

wlan tx-power auto interval

The **wlan tx-power auto interva**l Global Configuration mode command configures the recalculation Auto Transmit Power period. To restore defaults, use the **no** form of this command.

Syntax

wlan tx-power auto interval *minutes*

no wlan tx-power auto interval

Parameters

- *minutes* — Specifies the recalculation period, in minutes. (Range: 1–15000 minutes)

Default Configuration

The default recalculation period is 10 minutes.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the recalculation Auto Transmit Power period to 1200 minutes.

```
Console (config)# wlan tx-power auto interval 1200
```

wlan tx-power auto signal-strength

The **wlan tx-power auto signal-strength** Global Configuration mode command configures the target signal strength heard at the second-closest AP. To restore defaults, use the **no** form of this command.

Syntax

wlan tx-power auto signal-strength *dbm*

no wlan tx-power auto signal-strength

Parameters

- *dbm* — Specifies the signal strength, in dBm. (Range: -40 dBm – -80 dBm)

Default Configuration

The default target signal strength is -68 dBm.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the target signal strength heard at the second-closest AP to -50 dBm.

```
Console (config)# wlan tx-power auto signal-strength -50
```

wlan tx-power auto signal-loss

The **wlan tx-power auto signal-loss** Global Configuration mode command configures the minimum signal loss difference (transmitted-received) below which two AP radios are considered too close. To restore defaults, use the **no** form of this command.

Syntax

wlan tx-power auto signal-loss *db*

no wlan tx-power auto signal-loss

Parameters

- *db* — Specifies the signal loss, in dB. (Range: 20-80 dB)

Default Configuration

The default minimum signal loss difference is 60 dB.

Command Mode

Global Configuration mode

User Guidelines

The Auto Transmit Power algorithm adjusts AP power due to another AP which is very close, because it is impossible to avoid interference in that case and the APs will have essentially the same coverage zone. The minimum signal loss is the signal strength difference (transmitted - received) below which two radios are considered too close.

Example

The following example configures the minimum signal loss difference to 30 dB.

```
Console (config)# wlan tx-power auto signal-loss 30
```

wlan station idle-timeout

The **wlan station idle-timeout** Global Configuration mode command configures the length of time before an idle station is removed from the system and required to login. To restore defaults, use the **no** form of this command.

Syntax

wlan station idle-timeout *minutes*

no wlan station idle-timeout

Parameters

- *minutes* — Specifies the IDLE timeout in minutes. (Range: 3-1440)

Default Configuration

The default timeout is 30 minutes.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the length of time before an idle station is removed from the system and required to login, to 10 minutes.

```
Console (config)# wlan station idle-timeout 10
```

clear wlan station

The **clear wlan station** Privileged EXEC mode command disassociates a station.

Syntax

c**lear wlan station** *mac-address*

Parameters

- *mac-address* — The station MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disassociates a station with the MAC address 00-9E-92-4C-73-FC.

```
Console# clear wlan station 00-9E-92-4C-73-FC
```

show wlan

The **show wlan** Privileged EXEC mode displays information on the WLAN configuration.

Syntax

show wlan

Parameters

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the WLAN information for user called ‘Device’.

```
console# show wlan aps Device

NAME: Device
MAC Address: 00:f0:00:00:06:25
Type: a, g
State: Active
802.11a Radio: Enabled
802.11g Radio: Enabled
VLANs Allowed: 2, 3, 4, 5, 66, 77, 88, 99, 221, 224, 226, 666,
1000
Native VLAN: 1
Tunnel Source State: Enabled
Tunnel Priority: 39
IP Address: 1.1.1.11
DNS Name:
WAN Timing Constraints: Enabled
Console Logging: Enabled
console#
```

show wlan auto-tx-power

The **show wlan auto-tx-power** Privileged EXEC mode command displays information on the WLAN automatic power transmission configuration.

Syntax

show wlan auto-tx-power

Parameters

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on the WLAN automatic power transmission configuration.

```
Console # show wlan auto-tx-power

Automatic Transmit Power is enabled
Interval: 10 minutes
Signal Strength: -68 dBm
Signal Loss: 60 dB
```

show wlan logging configuration

The **show wlan logging configuration** Privileged EXEC mode command displays information on the WLAN logging configuration.

Syntax

show wlan logging configuration

Parameters

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on the WLAN logging configuration.

```
Console # show wlan logging configuration

Station authorized: Disabled
Station unauthorized: Disabled
Station deletion: Disabled
Station roaming: Enabled
```

show wlan stations

The **show wlan stations** Privileged EXEC mode command displays information on WLAN stations.

Syntax

show wlan stations [**mac** *mac-address* | **ap** *name*]

Parameters

- **mac** *mac-address* — The station's MAC address.
- **ap** *name* — The AP name (Range: 1 - 32 characters).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on WLANs.

```
Console# show wlan stations


MAC Address         State       SSID        AP      Session Time
----------          ------      -------     ------  ---------
00-9E-93-82-83-91   Authorized  Enterprise  AP1(g)  1d 03:08:58
00-9E-93-82-83-92   Authorized  Enterprise  AP2(g)  08:19:17
```

show wlan stations counters

The **show wlan stations counters** Privileged EXEC mode command displays information on WLAN stations traffic.

Syntax

show wlan stations counters [**mac** *mac-address*]

Parameters

- **mac** *mac-address* — The station's MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on WLAN stations.

```
Console# show wlan stations counters

Number of stations: 2

MAC Address         InPkts      OutPkts     MIC Errors
----------          ------      -------     ---------
00-9E-93-82-83-91   183892      1289        0
00-9E-93-82-83-92   128977      5327        0

console# show wlan stations counters mac 00:0e:35:63:5c:a7

MAC Address         InPkts      OutPkts     MIC Errors
-----------------   ------      -------     ---------
00:0e:35:63:5c:a7   13264       8           0
```

37 TROUBLESHOOTING

This section describes problems that may arise when installing the device and how to resolve these issues. This section includes the following topics:

- **Problem Managemen**t — Provides information about problem management with the devices.
- **Troubleshooting Solutions** — Provides a list of troubleshooting issues and solutions for using the devices.

Problem Management

Problem management includes isolating and quantifying problems, and applying solutions.

When a problem is detected, the exact nature of the problem must be determined. Problem analysis includes how the problem is detected, and what are its possible causes. With the problem known, the effects of the problem are recorded, including all known results of the problem. Once the problem is quantified, theappropriate solution can be applied. Solutions to common troubleshooting issues are found either in this document, or can be obtained through Customer Support.

If no solution is found in this document, please contact Customer Support for advice and instructions.

Troubleshooting Solutions

Listed below are possible troubleshooting problems and their solutions. These error messages include:

- Cannot connect to management using RS-232 serial connection
- Cannot connect to switch management using Telnet, HTTP, SNMP, etc.
- Self-test exceeds 15 seconds.
- No connection is established and the port LED is on.
- Device is in a reboot loop

- No connection and the port LED is off
- Add and Edit pages do not open.
- Lost password

Problem	Possible Cause	Solution
Cannot connect to management using RS-232 serial connection		Ensure the terminal emulator program is set to VT-100 compatible, 9600 baud rate, no parity, 8 data bits and one stop bit. Use the included cable, or ensure that the pin-out complies with a standard null-modem cable.
Cannot connect to switch management using Telnet, HTTP, SNMP, etc.		Ensure that the switch has a valid IP address, subnet mask and a configured default gateway. Check that your cable is properly connected with a valid link light, and that the port has not been disabled. Ensure that your management station is plugged into the appropriate VLAN to manage the device. If you cannot connect using Telnet or the web, the maximum number of connections may already be open. Please try again at a later time.
No response from the terminal emulation software	Faulty serial cable	Replace the serial cable.
	Incorrect serial cable	Replace the serial cable for a pin-to-pin straight/flat cable.

Problem	**Possible Cause**	**Solution**
	Software settings	Reconfigure the emulation software connection settings.
Response from the terminal emulations software is not readable.	Faulty serial cable	Replace the serial cable.
	Software settings	Reconfigure the emulation software connection settings.
Self-test exceeds 15 seconds.	The device may not be correctly installed.	Remove and reinstall the device. If that does not help, consult your technical support representative.
No connection is established and the port LED is on.	Wrong network address in the workstation.	Configure the network address in the workstation.
	No network address set.	Configure the network address in the workstation.
	Wrong or missing protocol.	Configure the workstation with IP protocol.
	Faulty ethernet cable.	Replace the cable.
	Faulty port.	Replace the module.
	Faulty module.	Replace the module.
	Incorrect initial configuration.	Erase the connection and reconfigure the port.
Device is in a reboot loop	Software fault	Download and install another working or previous software version from the console

Problem	Possible Cause	Solution
No connection and the port LED is off	Incorrect ethernet cable, e.g., crossed rather than straight cable, or vice versa, split pair (incorrect twisting of pairs).	Check pinout and replace if necessary.
	Fiber optical cable connection is reversed.	Change if necessary. Check Rx and Tx on the fiber-optic cable.
	Bad cable.	Replace with a tested cable.
	Wrong cable type.	Verify that all 10 Mbps connections use a Cat 5 cable.
		Check the port LED or zoom screen in the NMS application, and change settings if necessary.

Problem	**Possible Cause**	**Solution**
Add and Edit pages do not open.	A pop-up blocker is enabled.	Disable pop-up blockers.

Problem	Possible Cause	Solution

Lost password		The Password Recovery Procedure enables the user to override the current password configuration, and disables the need for a password to access the console.
		The password recovery is effective until the device is reset. If the password/user name has been forgotten or lost, the password must be reconfigured using either the CLI commands or via the Embedded Web Interface.
		The Password Recovery Procedure is invoked from the Startup menu:
		Reboot the system either by disconnecting the power supply, or enter the command: the following message is displayed:
		`Console #reload`
		`Are you sure you want to reboot the system (y/n)[n]?`
		Enter Y. The device reboots. After the POST, when the text “`Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.`” is displayed, press **<Enter>**. The Startup Menu is displayed.
		[1] Download software
		[2] Erase flash file
		[3] Erase flash sectors
		[4] Password Recovery Procedure
		[5] Enter Diagnostic Mode